Invariantentheorie

Prof. Dr. Holger Brenner
Universität Osnabrück
Fachbereich Mathematik/Informatik

Wintersemester 2012/2013

Inhaltsverzeichnis

Vorwort

1. Vorlesung - Einführende Beispiele

Wir beginnen mit einigen typischen Beispielen zur Invariantentheorie.

Dreieckskongruenzen

Beispiel 1.1. Wir betrachten Dreiecke im $\mathbb{R}^2$. Die Ebene $\mathbb{R}^2$ sei mit dem Standardskalarprodukt versehen, so dass wir Längen, Winkel und Flächeninhalte zur Verfügung haben. Eine *affine Isometrie* (oder eine *Kongruenz*) der Ebene ist eine Abbildung

$$\mathbb{R}^2 \longrightarrow \mathbb{R}^2$$

der Form

$$P \mapsto AP + v\,,$$

wobei $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ eine lineare Isometrie ist, also durch eine orthogonale Matrix beschrieben wird, und wobei $v \in \mathbb{R}^2$ ein (Verschiebungs)-Vektor ist. In Koordinaten liegt also die Abbildung

$$\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} v_1 \\ v_2 \end{pmatrix}$$

vor. Orthogonal bedeutet, dass die Spaltenvektoren eine Orthonormalbasis bilden. Im zweidimensionalen bedeutet dies, dass entweder A eine Drehmatrix

$$A = \begin{pmatrix} \cos\,\alpha & -\sin\,\alpha \\ \sin\,\alpha & \cos\,\alpha \end{pmatrix}$$

oder eine *gespiegelte Drehmatrix* (oder *uneigentliche Drehmatrix*)

$$A = \begin{pmatrix} \cos\,\alpha & \sin\,\alpha \\ \sin\,\alpha & -\cos\,\alpha \end{pmatrix}$$

ist. Zu den ebenen Kongruenzen gehören insbesondere *Verschiebungen*, *Achsenspiegelungen*, *Punktspiegelungen* und *Drehungen*, die auch aus der Schule bekannt sind. Diese Abbildungen erhalten allesamt das Skalarprodukt, Längen, Winkel (aber ohne die Orientierung) und Flächeninhalte.

Unter einem *Dreieck* in der Ebene verstehen wir einfach ein Tupel aus drei Punkten der Ebene, also ein geordnetes Tripel (P_1, P_2, P_3) mit $P_i = (x_i, y_i)$. Die Dreieckspunkte sind also geordnet und wir erlauben auch *degenerierte* (oder *ausgeartete*) Dreiecke, beispielsweise können die Punkte *kolinear* sein oder auch zusammenfallen. Eine Kongruenz g überführt ein Dreieck $\triangle$ in ein neues Dreieck, und zwar ist das Bilddreieck durch

$$g(\triangle) \;=\; g\,(P_1, P_2, P_3) \;=\; (g(P_1), g(P_2), g(P_3))$$

definiert. Zwei Dreiecke $\triangle_1$ und $\triangle_2$ heißen *geordnet kongruent*, wenn es eine Kongruenz gibt, die das eine Dreieck in das andere überführt (bei einer nicht geordneten Kongruenz kann man noch die Nummerierung der Punkte

ändern). Die (geordnete) Kongruenz von Dreiecken ist eine Äquivalenzrelation. Unter einer Kongruenz bleiben diejenigen Größen eines Dreiecks erhalten, die generell unter einer Kongruenz erhalten bleiben, also der Flächeninhalt, die Länge der Seiten, und daraus abgeleitete Größen wie der Umfang des Dreiecks, die Länge der kleinsten Seite, usw., dagegen werden andere Größen des Dreiecks verändert, seine Lage im Raum, die Koordinaten seiner Punkte.

Da ein Dreieck durch die Koordinaten seiner Eckpunkte vollständig beschrieben wird, müssen alle dem Dreieck zugeordneten Größen als eine Funktion der sechs Koordinaten $(x_1, y_1, x_2, y_2, x_3, y_3)$ ausdrückbar sein. Eine Größe ist also einfach eine zunächst beliebige Funktion

$$\mu\colon \mathbb{R}^6 \longrightarrow \mathbb{R},\ \triangle \longmapsto \mu(\triangle),$$

(man kann auch andere Wertebereiche zulassen). Man sagt, dass eine solche Funktion *nur von der Kongruenzklasse abhängt* oder *invariant* unter der Kongruenz ist, wenn für jedes Dreieck $\triangle \in \mathbb{R}^6$ und jede Kongruenz g die Gleichheit

$$\mu(\triangle) \;=\; \mu(g(\triangle))$$

gilt. Eine solche invariante Funktion nennt man auch eine *innere Größe* des Dreiecks, da sie nicht von der Lage des Dreiecks in der Ebene abhängt (wobei man sowohl die invariante Funktion als auch den Wert einer solchen an einem bestimmten Dreieck als innere Größe bezeichnet).

Der Flächeninhalt (vergleiche Aufgabe 1.1; man verschiebe den Eckpunkt (x_3, y_3) des Dreiecks in den Nullpunkt und betrachte dann die daran anliegenden Seiten als Vektoren) des Dreiecks wird durch

$$\begin{aligned}
\mu(\triangle) &= \frac{1}{2}\left|\det\begin{pmatrix} x_1 - x_3 & x_2 - x_3 \\ y_1 - y_3 & y_2 - y_3 \end{pmatrix}\right| \\
&= \frac{1}{2}\left|(x_1 - x_3)\,(y_2 - y_3) - (y_1 - y_3)\,(x_2 - x_3)\right| \\
&= \frac{1}{2}\left|x_1y_2 - x_2y_1 - x_1y_3 + x_3y_1 - x_3y_2 + x_2y_3\right|
\end{aligned}$$

gegeben. Aufgrund der inhaltlichen Interpretation als Flächeninhalt eines Dreiecks muss es sich um eine innere Größe handeln. Dies lässt sich aber auch numerisch überprüfen. Um den Rechenaufwand zu minimieren, sind folgende einfache Vorüberlegungen sinnvoll:

• Wenn eine Funktion μ invariant ist, so ist auch jede Funktion invariant, die nur von dieser Funktion abhängt; wenn also der Ausdruck $\nu(\triangle) = x_1y_2 - x_2y_1 - x_1y_3 + x_3y_1 - x_3y_2 + x_2y_3$ unter einer bestimmten Kongruenz invariant ist, so ist insbesondere auch der Betrag davon unter dieser Kongruenz invariant.

• Da man jede Kongruenz als Hintereinanderschaltung von besonders einfachen Kongruenzen schreiben kann, nämlich von Verschiebungen, Drehungen

und eventuell einer Spiegelung an der x-Achse, genügt es, die Invarianz unter diesen erzeugenden Kongruenzen zu zeigen.

Betrachten wir also diese speziellen Kongruenzen. Bei einer Verschiebung g um den Vektor $(w,\, z)$ ist

$$\begin{aligned}\nu(g(\triangle)) &= \nu\left(x_1+w,\, y_1+z,\, x_2+w,\, y_2+z,\, x_3+w,\, y_3+z\right)\\ &= \det\begin{pmatrix} x_1-w-(x_3-w) & x_2-w-(x_3-w)\\ y_1-z-(y_3-z) & y_2-z-(y_3-z)\end{pmatrix}\\ &= \det\begin{pmatrix} x_1-x_3 & x_2-x_3\\ y_1-y_3 & y_2-y_3\end{pmatrix}\\ &= \nu(\triangle).\end{aligned}$$

Für eine Drehung D um den Winkel α und einen Vektor $v \in V$ und die zugehörige Verschiebung V_v gilt $V_{-D(v)} \circ D \circ V_v = D$. Da wir die Invarianz unter einer Verschiebung schon bewiesen haben, können wir annehmen, dass der dritte Eckpunkt der Nullpunkt ist, dass also $(x_3, y_3) = (0, 0)$ ist. Damit ist aufgrund des Determinantenmultiplikationssatzes

$$\begin{aligned}\nu(D(\triangle)) &= \det\left(\begin{pmatrix}\cos\alpha & -\sin\alpha\\ \sin\alpha & \cos\alpha\end{pmatrix}\begin{pmatrix} x_1 & x_2\\ y_1 & y_2\end{pmatrix}\right)\\ &= \det\begin{pmatrix}\cos\alpha & -\sin\alpha\\ \sin\alpha & \cos\alpha\end{pmatrix}\det\begin{pmatrix} x_1 & x_2\\ y_1 & y_2\end{pmatrix}\\ &= \det\begin{pmatrix} x_1 & x_2\\ y_1 & y_2\end{pmatrix}\\ &= \nu(\triangle).\end{aligned}$$

Für die Spiegelung $S = \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$ ist schließlich

$$\nu(S(\triangle)) = \nu\left(\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}\begin{pmatrix} x_1-x_3 & x_2-x_3\\ y_1-y_3 & y_2-y_3\end{pmatrix}\right) = -\nu(\triangle).$$

Die Funktion ν ist also nicht invariant unter der Spiegelung, wohl aber ihr Betrag oder das Quadrat davon (letzteres gilt über jedem Körper). Die Funktion ν (oder ν^2 oder $|\nu|$) enthält auch die Information, ob das Dreieck ausgeartet ist oder nicht, nämlich genau dann, wenn ν den Wert 0 annimmt.

Betrachten wir die Seitenlängen. Da wir mit geordneten Dreiecken arbeiten, sind (für $i \neq j$) die Seitenlängen

$$L_{ij} = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2}$$

invariant unter Kongruenzen (sie sind nicht invariant unter Umnummerierungen, da diese ja beispielsweise L_{12} in L_{13} überführen). Der Ausdruck $U = L_{12} + L_{13} + L_{23}$, also der Umfang, ist invariant unter den Kongruenzen, aber auch unter Umnummerierungen.

Die Invarianz der Seitenlängen ist ein Spezialfall der Invarianz der Skalarprodukte. Isometrien erhalten das Skalarprodukt, dies ist ihre definierende

Eigenschaft. Zu $i \neq j$ (und k die dritte Zahl aus $\{1,2,3\}$) sei

$$\begin{aligned} S_{ij} &:= \left\langle \begin{pmatrix} x_i - x_k \\ y_i - y_k \end{pmatrix}, \begin{pmatrix} x_j - x_k \\ y_j - y_k \end{pmatrix} \right\rangle \\ &= (x_i - x_k)(x_j - x_k) + (y_i - y_k)(y_j - y_k) \\ &= x_i x_j - x_i x_k - x_j x_k + x_k^2 + y_i y_j - y_i y_k - y_j y_k + y_k^2. \end{aligned}$$

Das ist also das Skalarprodukt der beiden vektoriellen Seiten, die am Eckpunkt P_k anliegen. Diese Funktionen sind invariant unter geordneten Kongruenzen. Die Invarianz der Winkel (an einer bestimmten Ecke) zwischen zwei Dreiecksseiten folgt direkt aus der Invarianz der Skalarprodukte der zwei Seiten.

Es gibt eine Reihe von elementargeometrischen Sätzen, die besagen, dass ein Dreieck bis auf Kongruenz durch die Angabe gewisser Größen bestimmt ist, z.B. durch die Angabe der drei Seitenlängen oder die Angabe eines Winkels und der Längen der beiden anliegenden Seiten. Betrachten wir die drei Längen als Abbildung (die wir die *Längenabbildung* nennen)

$$L\colon \mathbb{R}^6 \longrightarrow \mathbb{R}^3,\ \triangle \longmapsto (L_{12}(\triangle),\ L_{13}(\triangle),\ L_{23}(\triangle))\,.$$

Zwei Dreiecke sind genau dann kongruent, wenn ihre Werte unter der Abbildung L übereinstimmen. Die Faser der Abbildung über einem Längentupel ℓ_1, ℓ_2, ℓ_3 besteht aus allen geordneten Dreiecken, deren Seitenlängen gleich ℓ_i sind. Die Abbildung ist nicht surjektiv, da das Längentupel eines Dreiecks in $\mathbb{R}^3_{\geq 0}$ liegt und die Dreiecksungleichung $\ell_1 \leq \ell_2 + \ell_3$ (und Permutationen davon)erfüllen muss (über einem algebraisch abgeschlossenen Körper ist die Abbildung aber surjektiv). Wenn $\mu\colon \mathbb{R}^6 \to \mathbb{R}$ irgendeine invariante Funktion ist, so ist diese auf den Kongruenzklassen, also den Fasern von L, konstant, und somit gibt es eine eindeutig bestimmte Funktion $\tilde{\mu}\colon \mathbb{R}^3 \to \mathbb{R}$ mit $\mu = \tilde{\mu} \circ L$. In einem gewissen Sinn beschreiben die L_{ij} sämtliche invarianten Funktionen.

Symmetrische Polynome

Definition 1.2. Es sei K ein Körper. Ein Polynom $f \in K[X_1, \ldots, X_n]$ heißt *symmetrisch*, wenn für jede Permutation $\sigma \in S_n$ die Gleichheit

$$f = f^\sigma$$

besteht, wobei f^σ aus f entsteht, indem man überall in f die Variable X_i durch $X_{\sigma(i)}$ ersetzt.[1]

[1]Wenn man die durch eine Permutation induzierte lineare Abbildung

$$K^n \longrightarrow K^n,\ e_i \longmapsto e_{\sigma(i)},$$

betrachtet, so ist es natürlicher, die i-te Variable X_i, die ja die i-te Projektion von K^n auf K bezeichnet, auf $X_i \circ \sigma$, also auf $X_{\sigma^{-1}(i)}$, abzubilden.

Beispiel 1.3. Bei $n = 1$ sind alle Polynome symmetrisch, da dort allein die Identität vorliegt. Bei $n = 2$ sind die Konstanten und beispielsweise $x + y, xy, 5 + x + y, 3x + 3y + x^2y^2$ symmetrische Polynome. Bei $n = 3$ sind $x + y + z$, $xy + xz + yz$, xyz, $x^4 + y^4 + z^4$ typische Beispiele.

Die Summe und das Produkt von symmetrischen Polynomen ist wieder symmetrisch, daher bilden die symmetrischen Polynome einen Unterring des Polynomringes.

Definition 1.4. Das i-te *elementarsymmetrische Polynom* in n Variablen ist das Polynom (mit $i = 1, \ldots, n$)

$$E_i := \sum_{1 \leq k_1 < \ldots < k_i \leq n} X_{k_1} \cdots X_{k_i}.$$

Die elementarsymmetrischen Polynome treten in folgender Situation auf.

Bemerkung 1.5. Wir betrachten das Produkt

$$(T + X_1) \ldots (T + X_n)$$

in $K[X_1, \ldots, X_n, T] = K[X_1, \ldots, X_n][T]$. Wenn man dieses Produkt ausmultipliziert, so erhält man ein (normiertes) Polynom in T vom Grad n, wobei die Koeffizienten selbst Polynome aus $K[X_1, \ldots, X_n]$ sind. Da man beim Ausmultiplizieren alles mit allem multiplizieren muss, gilt

$$(T + X_1) \cdots (T + X_n) = T^n + E_1 T^{n-1} + \ldots + E_n T^0,$$

wobei E_i gerade das i-te elementarsymmetrische Polynom bezeichnet. Ein Polynom in T mit den Nullstellen $-X_i$ besitzt also die elementarsymmetrischen Polynome als Koeffizienten.

Mit Hilfe der elementarsymmetrischen Polynome kann man nun einfach alle symmetrischen Polynome in eindeutiger Form schreiben. Dies ist der Inhalt des *Hauptsatzes über symmetrische Polynome*. Für den Beweis benötigen wir den Begriff der *gradlexikographischen Ordnung*.

Definition 1.6. Es sei K ein Körper und $K[X_1, \ldots, X_n]$ der Polynomring über K. Die *gradlexikographische Ordnung* auf der Menge der Monome ist durch

$$X_1^{a_1} \cdots X_n^{a_n} \prec X_1^{b_1} \cdots X_n^{b_n},$$

falls der Grad von $X_1^{a_1} \cdots X_n^{a_n}$, (also $\sum_{i=1}^n a_i$), kleiner als der Grad von $X_1^{b_1} \cdots X_n^{b_n}$ ist, oder, bei gleichem Grad, wenn $a_1 = b_1, \ldots, a_k = b_k$, aber $a_{k+1} < b_{k+1}$ ist, gegeben.

Man verwendet also die Ordnung auf der Variablenmenge. Man vergleicht zwei Monome f und g, indem man zuerst den Grad miteinander vergleicht. Stimmt dieser überein, so vergleicht man die Exponenten der ersten Variable

der beiden Monome miteinander (man vergleicht also den „Anfangsbuchstaben“). Wenn es hier einen Größenunterschied gibt, so ist die Sache entschieden. Andernfalls schaut man sich den Exponenten der zweiten Variablen an, und so weiter. Dies führt zu einer totalen Ordung auf der Menge der Monome. Zu einem Monom gibt es jeweils nur endlich viele Monome, die bezüglich dieser Ordnung kleiner sind. Daher kann man über diese Ordnung Induktion führen.

Zu einem Polynom f nennt man das Monom aus f (mit einem Koeffizienten $\neq 0$) mit dem größten Exponententupel in der gradlexikographischen Ordnung das *Leitmonom* von f.

Satz 1.7. *Jedes symmetrische Polynom $F \in K[X_1, \ldots, X_n]$ lässt sich eindeutig als Polynom in den elementarsymmetrischen Polynomen schreiben. D.h. es ist*

$$F = \sum_{\nu} a_\nu E^\nu$$

mit eindeutig bestimmten Koeffizienten $a_\nu \in K$.

Beweis. Wir führen Induktion über die gradlexikographische Ordnung. Zur Existenz. Es sei F ein symmetrisches Polynom. Es sei $X_1^{a_1} \cdots X_n^{a_n}$ das Leitmonom von F (mit dem Koeffizienten $c \neq 0$) Es ist $a_{i+1} \leq a_i$ für alle i. Andernfalls nämlich betrachtet man die Permutation, die X_{i+1} und X_i vertauscht. Das resultierende Monom muss wegen der Symmetrie ebenfalls in F vorkommen, wäre aber größer in der gradlexikographischen Ordnung.

Wir betrachten das Polynom

$$G = F - cE_1^{a_1-a_2} E_2^{a_2-a_3} \cdots E_{n-1}^{a_{n-1}-a_n} E_n^{a_n}.$$

Dabei treten rechts die elementarsymmetrischen Polynome mit nichtnegativen Exponenten auf. Das Polynom rechts enthält ebenfalls $X_1^{a_1} \cdots X_n^{a_n}$ als Leitmonom: Hierzu muss man sich die Monome in E_i klar machen. Das Leitmonom von E_i ist $X_1 \cdots X_i$ und das Leitmonom von E_i^k ist $(X_1 \cdots X_i)^k$ (das Leitmonom ist multiplikativ, siehe Aufgabe 1.10). Daher hat das Polynom rechts das Leitmonom

$$X_1^{a_1-a_2} \cdot (X_1X_2)^{a_2-a_3} \cdots (X_1 \cdots X_{n-1})^{a_{n-1}-a_n} \cdot (X_1 \cdots X_n)^{a_n} = X_1^{a_1} X_2^{a_2} \cdots X_{n-1}^{a_{n-1}} X_n^{a_n}.$$

In der Differenz G verschwindet also dieses Monom, d.h. G hat einen kleineren Grad in der gradlexikographischen Ordung. Da G ebenfalls symmetrisch ist, liefert die Induktionsvoraussetzung die Behauptung. Zur Eindeutigkeit. Wir zeigen, dass die elementarsymmetrischen Polynome algebraisch unabhängig sind. Sei also

$$H(E_1, \ldots, E_n) = 0,$$

wobei $H \neq 0$ ein Polynom in den n Variablen $Y_1, \ldots, Y_n$ sei. Wir schreiben H als Summe von Monomen der Form

$$Y_1^{a_1-a_2} Y_2^{a_2-a_3} \cdots Y_n^{a_n}$$

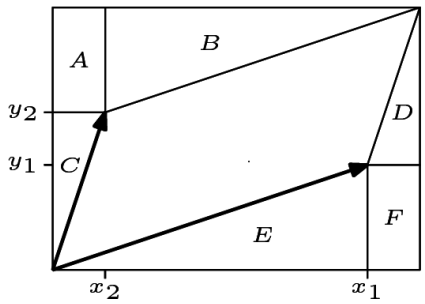
mit $a_1 \geq \ldots \geq a_n$. Es sei $(a_1, \ldots, a_n)$ dasjenige Tupel mit $a_i \geq a_{i+1}$, das in der gradlexikographischen Ordnung maximal ist unter allen Tupeln, für die $Y_1^{a_1-a_2} Y_2^{a_2-a_3} \cdots Y_n^{a_n}$ in H vorkommt (es werden also die a verglichen, nicht die Differenzen). Dann besitzt $H(E_1, \ldots, E_n)$ als Polynom in X das Leitmonom $X_1^{a_1} \cdots X_n^{a_n}$ und wäre nicht 0. □

Insbesondere ist der Ring der symmetrischen Polynome selbst isomorph zu einem Polynomring in n Variablen.

1. Arbeitsblatt

Aufwärmaufgaben

Aufgabe 1.1. Man mache sich anhand des Bildes klar, dass zu zwei Vektoren (x_1, y_1) und (x_2, y_2) die Determinante der durch die Vektoren definierten 2×2-Matrix mit dem Flächeninhalt des von den beiden Vektoren aufgespannten *Parallelogramms* (bis auf das Vorzeichen) übereinstimmt.



Aufgabe 1.2. Es seien $P_1 = (a_1, b_1)$, $P_2 = (a_2, b_2)$ und $P_3 = (a_3, b_3)$ drei Punkte im $\mathbb{R}^2$. Stelle den Flächeninhalt des zugehörigen Dreiecks mit a_1, b_1, a_2, b_2, a_3, b_3 dar.

Aufgabe 1.3. Drücke die Funktion ν^2 als Funktion der L_{ij}^2 (siehe Vorlesung) aus.

Aufgabe 1.4. Drücke die Funktion $S_{12}+S_{13}+S_{23}$ als Funktion der L_{ij}^2 (siehe Vorlesung) aus.

Aufgabe 1.5. Wir betrachten die Abbildung

$$\mathbb{R}^6 \longrightarrow \mathbb{R}^3, (x_1,\, y_1,\, x_2,\, y_2,\, x_2,\, y_2) \longmapsto$$
$$\left(\sqrt{(x_1-x_2)^2+(y_1-y_2)^2},\, \sqrt{(x_1-x_3)^2+(y_1-y_3)^2},\, \sqrt{(x_2-x_3)^2+(y_2-y_3)^2}\right),$$

die einem Dreieck die Längen seiner Seiten zuordnet. Zeige, dass das Bild dieser Abbildung die Punkte $(\ell_1,\, \ell_2,\, \ell_3) \in \mathbb{R}^3_{\geq 0}$ sind, die die Dreiecksungleichung erfüllen.

Aufgabe 1.6. Diskutiere die Ähnlichkeit von Dreiecken analog zu Beispiel 1.1.

Aufgabe 1.7. Wir fassen ein Dreieck $\triangle$ als ein geordnetes Tripel $(P_1, P_2, P_3) \in \mathbb{R}^6$ auf. Begründe die folgenden topologischen Eigenschaften.

(1) Die Menge der nichtentarteten Dreiecke ist offen.
(2) Die Menge der gleichseitigen Dreiecke ist abgeschlossen.
(3) Die Menge der gleichschenkligen Dreiecke ist abgeschlossen.

Aufgabe 1.8. Wir betrachten die Abbildung

$$\mathbb{R}^6 \longrightarrow \mathbb{R}^3, (x_1,\, y_1,\, x_2,\, y_2,\, x_2,\, y_2) \longmapsto$$
$$\left((x_1-x_2)^2+(y_1-y_2)^2,\, (x_1-x_3)^2+(y_1-y_3)^2,\, (x_2-x_3)^2+(y_2-y_3)^2\right),$$

die einem Dreieck die Längenquadrate seiner Seiten zuordnet. Bestimme die regulären Punkte der Abbildung.

Aufgabe 1.9. Es sei K ein Körper und sei $R = K[X_1, \ldots, X_n]$ der Polynomring über K. Zeige, dass ein Polynom $F \in R$ genau dann symmetrisch ist, wenn die homogenen Komponenten von F symmetrisch sind.

Aufgabe 1.10. Es sei K ein Körper und sei $R = K[X_1, \ldots, X_n]$ der Polynomring über K. Zu $f \in R$, $f \neq 0$, sei $\mathrm{LM}(f)$ das Leitmonom zu f in der gradlexikographischen Ordnung. Zeige, dass das Leitmonom sich multiplikativ verhält, dass also

$$\mathrm{LM}(fg) \;=\; \mathrm{LM}(f) \cdot \mathrm{LM}(g)$$

für Polynome $f, g \neq 0$ gilt.

Aufgabe 1.11. Schreibe das symmetrische Polynom

$$X^3Y^3 - 2X^2 - 2Y^2 + 5XY$$

als Polynom in den elementarsymmetrischen Polynomen.

Aufgabe 1.12. Schreibe das symmetrische Polynom

$$3X^2Y^2Z^2 - X^4 - Y^4 - Z^4 + X^3Y^3Z^3$$

als Polynom in den elementarsymmetrischen Polynomen.

Aufgabe 1.13. Schreibe die symmetrischen Polynome

$$X_1^k + \ldots + X_n^k$$

als Polynom in den elementarsymmetrischen Polynomen.

Aufgaben zum Abgeben

Aufgabe 1.14. (4 Punkte)

Bestimme die Fasern (bis auf Homöomorphie) der Längenabbildung L aus Beispiel 1.1.

Aufgabe 1.15. (5 Punkte)

Wir betrachten die Abbildung

$$\mathbb{R}^6 \longrightarrow \mathbb{R}^3, (x_1, y_1, x_2, y_2, x_2, y_2) \longmapsto \left(\sqrt{(x_1-x_2)^2+(y_1-y_2)^2}, \sqrt{(x_1-x_3)^2+(y_1-y_3)^2}, \sqrt{(x_2-x_3)^2+(y_2-y_3)^2}\right),$$

die einem Dreieck die Längen seiner Seiten zuordnet. Es sei B das Bild der Abbildung. Gibt es eine stetige Abbildung

$$s\colon\ B \longrightarrow \mathbb{R}^6$$

mit

$$L \circ s\ =\ \mathrm{Id}_B?$$

Aufgabe 1.16. (5 Punkte)

Es sei K ein algebraisch abgeschlossener Körper. Zeige, dass die Abbildung

$$K^6 \longrightarrow K^3, (x_1, y_1, x_2, y_2, x_2, y_2) \longmapsto \left((x_1-x_2)^2+(y_1-y_2)^2, (x_1-x_3)^2+(y_1-y_3)^2, (x_2-x_3)^2+(y_2-y_3)^2\right),$$

surjektiv ist.

Aufgabe 1.17. (3 Punkte)

Es sei K ein Körper, der eine dritte primitive Einheitswurzel ζ enthalte. Zeige, dass das Polynom

$$\left(X_1 + \zeta X_2 + \zeta^2 X_3\right)^3 \in K[X_1, X_2, X_3]$$

symmetrisch ist und bestimme seine Darstellung mit den elementarsymmetrischen Polynomen.

Aufgabe 1.18. (4 Punkte)

Bestimme die kritischen Punkte der durch die elementarsymmetrischen Polynome definierten Gesamtabbildung

$$\mathbb{R}^n \longrightarrow \mathbb{R}^n,\, (x_1, \ldots, x_n) \longmapsto (E_1(x_1, \ldots, x_n), \ldots, E_n(x_1, \ldots, x_n)).$$

2. Vorlesung - Operationen von Gruppen

Gruppenoperationen

In den beiden Beispielen der ersten Vorlesung operiert eine Gruppe auf einer Menge: Die Kongruenzabbildungen bilden eine Gruppe, und eine Kongruenz überführt ein Dreieck in ein weiteres (kongruentes) Dreieck. Eine Permutation $\sigma \in S_n$ überführt ein n-Tupel in ein weiteres Tupel und ein Polynom (in n Variablen) in ein Polynom über. Diese Situation wird durch den Begriff der Gruppenoperation erfasst, welcher grundlegend für die Invariantentheorie ist.

Es sei G eine zumeist multiplikativ geschriebene Gruppe mit neutralem Element e.

Definition 2.1. Es sei G eine Gruppe und M eine Menge. Eine Abbildung

$$G \times M \longrightarrow M,\, (g, x) \longmapsto gx,$$

heißt *Gruppenoperation* (von G auf M), wenn die beiden folgenden Eigenschaften gelten.

(1) $ex = x$ für alle $x \in M$.
(2) $(gh)x = g(hx)$ für alle $g, h \in G$ und für alle $x \in M$.

Man spricht auch von einer *Aktion* oder einer *Wirkung* der Gruppe G auf M. Im Zusammenhang von Gruppenoperationen schreibt man die Gruppe zumeist multiplikativ, und ebenso schreibt man die Operation multiplikativ.

Definition 2.2. Es sei G eine Gruppe und M eine Menge. Eine Gruppenoperation von G auf M heißt *treu*, wenn aus $gx = x$ für alle $x \in M$ folgt, dass $g = e$ ist.

Lemma 2.3. *Es sei G eine Gruppe und M eine Menge. Es sei* $\mathrm{Perm}(M)$ *die Gruppe der Permutationen auf M. Dann gelten folgende Aussagen.*

(1) *Wenn G auf M operiert, so ist die Abbildung*

$$G \longrightarrow \mathrm{Perm}\,(M),\ g \longmapsto (x \mapsto gx),$$

ein Gruppenhomomorphismus.

(2) *Wenn umgekehrt ein Gruppenhomomorphismus*

$$\varphi\colon\ G \longrightarrow \mathrm{Perm}\,(M),$$

vorliegt, so wird durch

$$G \times M \longrightarrow M,\ (g,x) \longmapsto (\varphi(g))(x),$$

eine Gruppenoperation von G auf M definiert.

Beweis. Siehe Aufgabe 2.1. □

Unter dieser Korrespondenz ist die Operation genau dann treu, wenn φ injektiv ist.

Beispiel 2.4. Nach Lemma 2.3 (2) und nach Lemma 4.4 (Körper- und Galoistheorie (Osnabrück 2011)) ist eine Gruppenoperation von $(\mathbb{Z}, 0, +)$ auf einer Menge M dasselbe wie eine bijektive Abbildung

$$F\colon\ M \longrightarrow M,$$

wobei die 1 wie F wirkt. Bei gegebenem F ist also die Gruppenwirkung für $x \in M$ durch

$$n \cdot x = F^n(x)$$

definiert, wobei F^n bei $n \geq 0$ die n-fache Hintereinanderschaltung von F und bei $n < 0$ die $-n$-fache Hintereinanderschaltung der Umkehrabbildung F^{-1} bedeutet.

Definition 2.5. Es liege eine Gruppenoperation einer Gruppe G auf einer Menge M vor. Man nennt zwei Elemente $x, y \in M$ *G-äquivalent* (oder äquivalent unter G), wenn es ein $g \in G$ mit $y = gx$ gibt.

Diese Relation ist in der Tat eine Äquivalenzrelation, wie man sich direkt überlegen kann. Die Äquivalenzklassen bekommen einen eigenen Namen.

Definition 2.6. Es liege eine Gruppenoperation einer Gruppe G auf einer Menge M vor. Die Äquivalenzklassen auf M zur G-Äquivalenz nennt man die *Bahnen der Operation*.

Definition 2.7. Es liege eine Gruppenoperation einer Gruppe G auf einer Menge M vor. Zu $x \in M$ heißt

$$G_x = \{g \in G |\, gx = x\}$$

die *Isotropiegruppe* zu x.

Dabei handelt es sich um eine Untergruppe von G. Andere Bezeichnungen hierfür sind *Standgruppe* oder *Stabilisator*.

Definition 2.8. Es liege eine Gruppenoperation einer Gruppe G auf einer Menge M vor. Ein Punkt $x \in M$ heißt *Fixpunkt der Operation*, wenn $gx = x$ ist für alle $g \in G$.

Ein Element $x \in M$ ist genau dann ein Fixpunkt der Operation, wenn die Bahn durch diesen Punkt einelementig ist, und dies ist genau dann der Fall, wenn die zugehörige Standgruppe ganz G ist.

Beispiel 2.9. Es sei G eine Gruppe und M eine Menge. Dann gibt es stets die sogenannte *triviale Operation* von G auf M, die durch $gx = x$ für alle $g \in G$ und alle $x \in M$ gegeben ist. In diesem Fall ist jeder Punkt ein Fixpunkt und alle Bahnen sind einelementig.

Definition 2.10. Es liege eine Gruppenoperation einer Gruppe G auf einer Menge M vor. Die Operation heißt *transitiv*, wenn es zu je zwei Elementen $x, y \in M$ ein $g \in G$ mit $gx = y$ gibt.

Eine Operation ist genau dann transitiv, wenn es nur eine Bahn gibt.

Beispiel 2.11. Sei G eine Gruppe. Die Verknüpfung

$$G \times G \longrightarrow G,\ (g,h) \longmapsto gh,$$

kann man als eine Gruppenoperation der Gruppe G auf sich selbst ansehen. Diese Operation ist treu und transitiv, es gibt also nur eine Bahn. Für zwei Elemente g_1 und g_2 ist ja $g_1 = (g_1 g_2^{-1})g_2$.

Beispiel 2.12. Sei G eine Gruppe und $H \subseteq G$ eine Untergruppe. Dann liefert die Verknüpfung

$$H \times G \longrightarrow G,\ (h,g) \longmapsto hg,$$

eine Gruppenoperation von H auf G. Die Bahnen dieser Operation stimmen mit den Rechtsnebenklassen zu dieser Untergruppe überein. Wenn G endlich ist, so sind die Bahnen (nach dem Beweis zu Satz 4.16 (Körper- und Galoistheorie (Osnabrück 2011))) alle gleichmächtig, was bei einer beliebigen Gruppenoperation keineswegs der Fall sein muss.

Beispiel 2.13. Sei $n \in \mathbb{N}$, $M = \{1, \ldots, n\}$ und S_n die Gruppe der Permutationen auf M. Dann liegt eine natürliche Operation

$$S_n \times M \longrightarrow M,\ (\sigma, i) \longmapsto \sigma(i),$$

vor. Der zugehörige Gruppenhomomorphismus ist die Identität. Die Operation ist treu, da jede Permutation $\neq \mathrm{id}_M$ mindestens ein Element aus M bewegt. Zu jedem $i \in M$ ist die Isotropiegruppe G_i isomorph zur Permutationsgruppe $S_{n-1} \cong \mathrm{Perm}\,(M \setminus \{i\})$. Für je zwei Elemente $i, j \in M$ gibt es eine Permutation (z.B. eine Transposition), die i in j überführt. Bei dieser Gruppenoperation gibt es also nur eine Bahn.

Beispiel 2.14. Es sei R ein kommutativer Ring und $G = R^\times$ seine Einheitengruppe. Die Einschränkung der Ringmultiplikation

$$R^\times \times R \longrightarrow R,\, (r,s) \longmapsto rs,$$

liefert eine Gruppenoperation der Einheitengruppe auf dem Ring. Diese Operation ist treu, das Nullelement ist ein Fixpunkt der Operation. Zwei Elemente $a, b \in R$, die bezüglich dieser Operation äquivalent sind, heißen assoziiert. Dieser Begriff spielt bei der eindeutigen Primfaktorzerlegung in einem faktoriellen Bereich eine wichtige Rolle.

Satz 2.15. *Es sei G eine endliche Gruppe, die auf einer endlichen Menge M operiere. Es sei F die Menge der Fixpunkte der Operation und es seien $G_1, \ldots, G_n$ die verschiedenen Bahnen mit mindestens zwei Elementen. Dann ist*

$$\#(M) \,=\, \#(F) + \sum_{i=1}^{n} \#(G_i).$$

Beweis. Die Menge M ist zerlegt in die Bahnen der Operation, und diese sind entweder einelementig und entsprechen den Fixpunkten, oder mehrelementig, und werden dann rechts mitgezählt. □

Beispiel 2.16. Sei G eine Gruppe. Die Konjugation kann man als eine Operation von G auf sich selbst auffassen, indem man

$$g \cdot x = gxg^{-1}$$

setzt. Dabei haben wir die Gruppenverknüpfung symbolfrei und die Operation zur Unterscheidung mit $\cdot$ geschrieben. Dass eine Operation vorliegt kann man direkt nachprüfen oder aus Lemma 5.2 (Körper- und Galoistheorie (Osnabrück 2011)) folgern. Die Äquivalenzklassen unter dieser Operation, also die Bahnen der Konjugation, heißen *Konjugationsklassen*. Die Elemente im Zentrum der Gruppe sind genau die Fixpunkte.

Beispiel 2.17. Es sei M eine Menge und

$$F\colon\, M \longrightarrow M$$

eine bijektive Abbildung mit der zugehörigen Gruppenoperation von $\mathbb{Z}$ auf M. Die Operation ist genau dann trivial, wenn F die Identität ist. Die Fixpunkte der Operation sind genau die Fixpunkte von F. Die Isotropiegruppe zu $x \in M$ ist $\mathbb{Z}k$ $(k \geq 1)$, falls x ein Fixpunkt der k-ten Hintereinanderschaltung F^k und k minimal mit dieser Eigenschaft ist; andernfalls ist sie gleich 0. Die durch $x \in M$ definierte Bahn besteht aus

$$\{F^n(x) |\, n \in \mathbb{Z}\}\ .$$

Dabei können natürlich einzelne Bahnen endlich sein, auch wenn die Operation treu ist.

Definition 2.18. Es liege eine Gruppenoperation einer Gruppe G auf einer Menge M vor. Dann nennt man die Menge der Bahnen den *Bahnenraum* der Operation. Er wird mit

$$M\backslash G$$

bezeichnet. Die Abbildung

$$M \longrightarrow M\backslash G,\, x \longmapsto [x],$$

wobei $[x]$ die Bahn durch x bezeichnet, heißt *Quotientenabbildung*.

Der Bahnenraum ist also einfach die Quotientenmenge der Äquivalenzrelation, die durch die Gruppenoperation festgelegt wird, und die angegebene Quotientenabbildung ist die zugehörige kanonische Projektion.

Beispiel 2.19. Wir betrachten die n-dimensionale Sphäre

$$S = \left\{x \in \mathbb{R}^{n+1} |\ ||x|| = 1\right\}$$

und die antipodale Abbildung

$$\alpha\colon\ S \longrightarrow S,\, x \longmapsto -x,$$

die also jeden Punkt auf seinen gegenüberliegenden Punkt abbildet. Wegen

$$\alpha \circ \alpha = \mathrm{Id}_S$$

gibt dies Anlass zu einer Operation von $G = \{1, -1\} \cong \mathbb{Z}/(2)$ auf der Sphäre S, bei der 1 durch die Identität und -1 durch α operiert. Diese Operation ist treu und jede Bahn ist zweielementig von der Form $\{x, -x\}$. Insbesondere besitzt die Operation keinen Fixpunkt. Der Bahnenraum (versehen mit einer geeigneten Topologie) heißt n-dimensionaler *reell-projektiver Raum*.

Definition 2.20. Sei G eine Gruppe und seien M und N zwei Mengen, auf denen jeweils G operiert. Dann heißt eine Abbildung

$$\varphi\colon\ M \longrightarrow N$$

G-invariant (oder *G-verträglich*) wenn für alle $g \in G$ und alle $x \in M$ die Gleichheit

$$\varphi(gx) = g\varphi(x)$$

gilt.

Dieser Begriff wird insbesondere auch dann verwendet, wenn die Gruppe G auf der zweiten Menge N trivial operiert.

Lemma 2.21. *Es liege eine Gruppenoperation einer Gruppe G auf einer Menge M vor. Es sei $M\backslash G$ der Bahnenraum zu dieser Operation. Dann gelten folgende Aussagen.*

(1) *Die Quotientenabbildung*

$$q\colon\ M \longrightarrow M\backslash G,\, x \longmapsto [x],$$

ist G-invariant (wobei G auf dem Bahnenraum trivial operiert).

(2) *Wenn N eine weitere Menge ist und*

$$\varphi\colon\ M \longrightarrow N$$

eine G-invariante Abbildung (wobei die Operation von G auf N trivial sei), so gibt es genau eine Abbildung

$$\tilde{\varphi}\colon\ M\backslash G \longrightarrow N$$

mit $\varphi = \tilde{\varphi} \circ q$.

Beweis. (1) Für $x \in M$ und $g \in G$ sind x und gx in der gleichen Äquivalenzklasse, also ist

$$q(gx) \ = \ [gx] \ = \ [x] \ = \ g[x].$$

(2) folgt aus Lemma 6.17 (Einführung in die Algebra (Osnabrück 2009)) (5).

□

Beispiel 2.22. Es sei X eine Menge und $n \in \mathbb{N}_+$. Wir setzen

$$M = X \times \cdots \times X$$

mit n Faktoren. Die Permutationsgruppe S_n operiert auf M durch

$$\sigma(x_1, \ldots, x_n) \ = \ \left(x_{\sigma(1)}, \ldots, x_{\sigma(n)}\right),$$

d.h. σ vertauscht die Indizes. Die Fixpunkte dieser Operation sind genau die Diagonalelemente, also die Elemente der Form $(y, \ldots, y)$. Wenn r die Anzahl der verschiedenen Elemente in $x \ = \ (x_1, \ldots, x_n)$ bezeichnet und a_i, $1 \leq i \leq r$, die Anzahl angibt, wie oft die einzelnen Werte auftreten, so ist die Isotropiegruppe zu x gleich $S_{a_1} \times \cdots \times S_{a_r}$ (das sind diejenigen Permutationen, die einen jeden Index auf einen Index mit gleichem Eintrag abbilden) und besitzt genau $a_1! \cdots a_r!$ Elemente. Die zugehörige Bahn besitzt entsprechend $\frac{n!}{a_1! \cdots a_r!}$ Elemente.

Bei $X = \mathbb{R}$ sind die polynomialen Funktionen

$$x_1 + \ldots + x_n, \sum_{i<j} x_i x_j, \ldots, x_1 \cdots x_n$$

(also die elementarsymetrischen Polynome) S_n-invariante Abbildungen nach $\mathbb{R}$.

Beispiel 2.23. Es liege eine Gruppenoperation einer Gruppe G auf einer Menge M vor. Es sei L eine weitere Menge und Abb (L, M) die Menge der Abbildungen von L nach M. Dann wird durch

$$G \times \text{Abb}\ (L, M) \longrightarrow \text{Abb}\ (L, M)\,,\ (g, \varphi) \longmapsto g\varphi,$$

wobei $g\varphi$ durch

$$(g\varphi)(x) = g(\varphi(x))$$

definiert sei, eine Operation von G auf Abb (L, M) gegeben. Für das neutrale Element $e \in G$ gilt ja

$$(e\varphi)(x) \;=\; e(\varphi(x)) \;=\; \varphi(x)$$

für jedes $x \in M$, also $e\varphi \;=\; \varphi$, und für beliebige $g, h \in G$, $\varphi \in$ Abb (L, M) und $x \in M$ gilt

$$((gh)\varphi)(x) \;=\; (gh)(\varphi(x)) \;=\; g(h(\varphi(x))) \;=\; g((h\varphi)(x)) \;=\; (g(h\varphi))(x),$$

also $(gh)\varphi \;=\; g(h\varphi)$.

Zu einer Gruppe G nennt man die Menge G mit der durch

$$g \cdot_{\mathrm{op}} h \;:=\; hg$$

definierten Verknüpfung die *oppositionelle Gruppe* zu G. Sie wird mit G^{op} bezeichnet.

Beispiel 2.24. Es liege eine Gruppenoperation einer Gruppe G auf einer Menge M vor. Es sei N eine weitere Menge und Abb (M, N) die Menge der Abbildungen von M nach N. Dann wird durch

$$G^{\mathrm{op}} \times \text{Abb}\,(M, N) \longrightarrow \text{Abb}\,(M, N)\,,\; (g, \varphi) \longmapsto g\varphi,$$

wobei $g\varphi$ durch

$$(g\varphi)(x) = (\varphi(gx))$$

definiert sei, eine Operation der oppositionellen Gruppe G^{op} auf Abb (M, N) gegeben. Für das neutrale Element $e \in G$ gilt ja

$$(e\varphi)(x) \;=\; \varphi(ex) \;=\; \varphi(x)$$

für jedes $x \in M$, also $e\varphi \;=\; \varphi$, und für beliebige $g, h \in G$, $\varphi \in$ Abb (M, N) und $x \in M$ gilt

$$\begin{aligned}((g \cdot_{\mathrm{op}} h)\varphi)(x) \;&=\; ((hg)\varphi)(x)\\ &=\; \varphi((hg)(x))\\ &=\; \varphi(h(gx))\\ &=\; (h\varphi)(gx) \;=\; (g(h\varphi))(x),\end{aligned}$$

also $(g \cdot_{\mathrm{op}} h)\varphi \;=\; g(h\varphi)$. Statt mit der oppositionellen Gruppe zu arbeiten kann man diese Konstruktion auch als eine Operation von rechts auffassen.

Die Fixelemente von Abb (M, N) unter dieser Operation sind gerade die G-invarianten Abbildungen von M nach N. Diese Konstruktion wird insbesondere bei $N = \mathbb{R}$ o.Ä. angewendet, wenn es also um auf M definierte Funktionen geht.

2. Arbeitsblatt

Aufwärmaufgaben

Aufgabe 2.1. Es sei G eine Gruppe und M eine Menge. Es sei $\mathrm{Perm}\,(M)$ die Gruppe der Permutationen auf M. Zeige folgende Aussagen.

(1) Wenn G auf M operiert, so ist die Abbildung
$$G \longrightarrow \mathrm{Perm}\,(M),\ g \longmapsto (x \mapsto gx),$$
ein Gruppenhomomorphismus.
(2) Wenn umgekehrt ein Gruppenhomomorphismus
$$\varphi\colon\ G \longrightarrow \mathrm{Perm}\,(M),$$
vorliegt, so wird durch
$$G \times M \longrightarrow M,\ (g,x) \longmapsto (\varphi(g))(x),$$
eine Gruppenoperation von G auf M definiert.

Aufgabe 2.2. Zeige, dass die G-Äquivalenz bei einer Gruppenoperation in der Tat eine Äquivalenzrelation ist.

Aufgabe 2.3. Bestimme für die Operation der Kongruenzen die Isotropiegruppen zu jedem Dreieck $\triangle = (P_1, P_2, P_3) \in \mathbb{R}^6$.

Aufgabe 2.4. Sei $n \in \mathbb{N}$. Betrachte die Gruppenoperation der n-ten Einheitswurzeln durch Multiplikation auf $\mathbb{C}$. Bestimme die Bahnen und die Isotropiegruppen dieser Operation. Kann man die Quotientenabbildung durch eine polynomiale Funktion realisieren?

Aufgabe 2.5. Es sei V ein endlichdimensionaler K-Vektorraum und $G = \mathrm{GL}(V)$ die allgemeine lineare Gruppe mit ihrer natürlichen Operation auf $V \setminus \{0\}$. Zeige, dass diese Gruppenoperation transitiv ist. Wie sieht es aus, wenn man $\mathrm{SL}(V)$ betrachtet?

Aufgabe 2.6. Es sei V ein n-dimensionaler K-Vektorraum und $G = \mathrm{GL}(V)$ die allgemeine lineare Gruppe zusammen mit ihrer natürlichen Operation auf der Menge
$$M = \{(v_1, \ldots, v_n) \in V^n | \,\mathrm{Basis}\}\ .$$
Zeige, dass diese Operation transitiv ist. Wie sieht es auf ganz V^n aus?

Aufgabe 2.7. Zeige, dass die Isotropiegruppe bei einer Gruppenoperation kein Normalteiler sein muss.

Aufgabe 2.8. Diskutiere Links- und Rechtsoperationen.

Aufgabe 2.9. Es sei X ein topologischer Raum und

$$R = C(X, \mathbb{R}) = \{f : X \longrightarrow \mathbb{R} | \, f \text{ stetige Abbildung}\}.$$

Zeige, dass R ein kommutativer Ring ist. Man gebe auch ein Beispiel an, das zeigt, dass R im Allgemeinen nicht nullteilerfrei ist.

Aufgabe 2.10. Es seien X und Y topologische Räume und

$$\varphi \colon X \longrightarrow Y$$

eine stetige Abbildung. Zeige, dass dies einen Ringhomomorphismus

$$C(Y, \mathbb{R}) \longrightarrow C(X, \mathbb{R}), \; f \longmapsto f \circ \varphi,$$

induziert.

Gemäß Aufgabe 2.1 ergibt eine Gruppenoperation für jedes $g \in G$ eine Bijektion $x \mapsto gx$ auf M. Wenn M zusätzliche Strukturen besitzt, so verlangt man häufig, dass diese Bijektionen diese Strukturen respektieren, also beispielsweise linear oder stetig sind. Man spricht dann von einer linearen oder von einer stetigen Operation oder sagt, dass die Gruppe als Gruppe von Automorphismen oder als Gruppe von Homöomorphismen operiert.

Aufgabe 2.11. Es sei X ein topologischer Raum, auf dem eine Gruppe G operiere, wobei zu jedem $g \in G$ die Abbildung $x \mapsto gx$ stetig sei. Zeige, dass dadurch eine Operation (von rechts) von G auf dem Ring der stetigen Funktionen $C(X, \mathbb{R})$ als Gruppe von Ringautomorphismen gegeben ist.

Aufgabe 2.12. Wir betrachten die geordneten Dreiecke $\triangle = (P_1, P_2, P_3)$ als Punkte im $\mathbb{R}^6$. Definiere eine Gruppenoperation der S_3 auf dem $\mathbb{R}^6$ derart, dass die Bahnen den ungeordneten Dreiecken (also den Dreiecken ohne Nummerierung) entsprechen. Bestimme die Isotropiegruppen zu jedem Dreieck.

Aufgabe 2.13. Zeige, dass zwei Permutationen $\sigma, \tau \in S_n$ genau dann konjugiert sind, wenn ihre Zykeldarstellung den gleichen Typ haben, d.h. wenn die Anzahl der Zykel und deren Längen übereinstimmen.

Aufgabe 2.14. Betrachte zur symmetrischen Gruppe S_n die Operation durch Konjugation. Bestimme die Bahnen und die Isotropiegruppen für $n \leq 5$.

Aufgabe 2.15. Es sei $\mathrm{GL}_n(K)$ die Menge der invertierbaren $n \times n$-Matrizen über einem Körper K. Zeige, dass für zueinander konjugierte Matrizen M und N aus $\mathrm{GL}_n(K)$ die folgenden Eigenschaften bzw. Invarianten übereinstimmen: Die Determinante, die Eigenwerte, die Dimension der Eigenräume zu einem Eigenwert, die Diagonalisierbarkeit, die Trigonalisierbarkeit.

Aufgaben zum Abgeben

Aufgabe 2.16. (4 Punkte)

Wir betrachten die geordneten Dreiecke $\triangle = (P_1, P_2, P_3)$ als Punkte im $\mathbb{R}^6$. Betrachte die Gruppenoperation der S_3 auf dem $\mathbb{R}^6$ durch Umnummerierung der Eckpunkte. Man gebe sechs reelle Polynome $(F_1, \ldots, F_6)$ an derart, dass die Fasern der dadurch definierten Gesamtabbildung

$$F\colon \mathbb{R}^6 \longrightarrow \mathbb{R}^6$$

genau die Bahnen der Operation sind.

Aufgabe 2.17. (3 Punkte)

Zeige, dass die reellen Zahlen $(\mathbb{R}, +)$ auf der Menge der komplexen Zahlen durch

$$\mathbb{R} \times \mathbb{C} \longrightarrow \mathbb{C},\ (t, z) \longmapsto e^{2\pi i t} z,$$

operiert. Bestimme die Bahnen, die Isotropiegruppen und die Quotientenabbildung dieser Operation.

Aufgabe 2.18. (3 Punkte)

Es sei

$$f\colon \mathbb{C} \longrightarrow \mathbb{C}$$

eine stetige Funktion. Zeige, dass die beiden folgenden Aussagen äquivalent sind.

(1) Es gibt eine stetige Funtion
$$g\colon \mathbb{R}_{\geq 0} \longrightarrow \mathbb{C}$$
mit $f(z) = g(|z|)$ für alle $z \in \mathbb{C}$.
(2) Für alle n-ten Einheitswurzeln $\zeta \in \mathbb{C}$ (alle $n \in \mathbb{N}$) ist $f(\zeta z) = f(z)$ für alle $z \in \mathbb{C}$.
(3) Für alle $w \in \mathbb{C}$ mit $|w| = 1$ ist $f(wz) = f(z)$ für alle $z \in \mathbb{C}$.

Aufgabe 2.19. (4 Punkte)

Wir betrachten die Menge der quadratischen Polynome

$$M = \left\{ aX^2 + bX + c | \, a, b, c \in K, \, a \neq 0 \right\}$$

über einem Körper K, und es sei G die Menge der Transformationen vom Typ $X \mapsto \alpha X + \beta$ mit $\alpha \neq 0$.

a) Zeige, dass G auf M in natürlicher Weise operiert.

b) Zeige, dass G auf K durch Multiplikation mit α^2 operiert.

c) Zeige, dass die *Diskriminante*, also der Ausdruck $b^2 - 4ac$, der einem quadratischen Polynom zugeordnet ist, G-verträglich bezüglich dieser beiden Operationen ist.

Aufgabe 2.20. (4 Punkte)

Bestimme die Konjugationsklassen der (eigentlichen) Würfelgruppe.

3. Vorlesung - Lineare Operationen

Eine Operation einer Gruppe G auf einer (geometrischen) Menge M ist das gleiche wie ein Gruppenhomomorphismus der Gruppe in die Permutationsgruppe des geometrischen Objektes. Häufig betrachtet man nur solche Operationen, deren zugehörige Permutationen *Automorphismen* sind, also die relevanten geometrischen Eigenschaften des Objektes respektieren. Bei einer Operation auf einer Mannigfaltigkeit wird man beispielsweise fordern, dass die Automorphismen Diffeomorphismen sind. Wenn das geometrische Objekt ein Vektorraum ist, so interessiert man sich insbesondere für die linearen Automorphismen.

Definition 3.1. Es sei K ein Körper und V ein K-Vektorraum. Es sei G eine Gruppe. Eine Operation

$$\mu \colon G \times V \longrightarrow V$$

heißt *linear*, wenn für jedes $\sigma \in G$ die Abbildung

$$V \longrightarrow V, \, v \longmapsto \mu(\sigma, v),$$

K-linear ist.

Bei einer linearen Operation sind die Abbildungen $\varphi_\sigma = \mu(\sigma, -)$ sogar K-Automorphismen. Eine lineare Operation ist das gleiche wie ein Gruppenhomomorphismus

$$G \longrightarrow \mathrm{GL}(V) \, .$$

Beispiel 3.2. Es sei V ein K-Vektorraum über einem Körper K. Die allgemeine lineare Gruppe $\mathrm{GL}(V)$ operiert in natürlicher Weise linear auf V. Die Elemente $\varphi \in \mathrm{GL}(V)$ sind ja definiert als K-Automorphismen von V in sich und somit ist die Abbildung

$$\mathrm{GL}(V) \times V \longrightarrow V,\ (\varphi, v) \longmapsto \varphi(v),$$

wohldefiniert. Da die Verknüpfung auf $\mathrm{GL}(V)$ einfach die Hintereinanderschaltung von Abbildungen ist, ergibt sich sofort

$$\varphi(\psi(v)) \ = \ (\varphi \circ \psi)(v),$$

so dass es sich um eine Gruppenoperation handelt. Diese Operation besitzt nur zwei Bahnen, nämlich den Nullpunkt 0 und $V \setminus \{0\}$, da es zu zwei von 0 verschiedenen Vektoren v_1 und v_2 stets einen Automorphismus gibt, der v_1 in v_2 überführt.

Beispiel 3.3. Es sei V ein K-Vektorraum über einem Körper K. Die natürliche lineare Operation der allgemeinen linearen Gruppe $\mathrm{GL}(V)$ auf V, also die Abbildung

$$\mathrm{GL}(V) \times V \longrightarrow V,\ (\varphi, v) \longmapsto \varphi(v),$$

induziert für jede Untergruppe $G \subseteq \mathrm{GL}(V)$ eine lineare Operation

$$G \times V \longrightarrow V,\ (\varphi, v) \longmapsto \varphi(v).$$

Diese einfache Konstruktion beinhaltet eine Vielzahl von interessanten Operationen. Wichtige Untergruppen der $\mathrm{GL}(V)$ sind die spezielle lineare Gruppe $\mathrm{SL}(V)$ (dazu muss V endlichdimensional sein) und alle endlichen Gruppen (wenn die Dimension von V hinreichend groß ist). Wenn der Vektorraum weitere Strukturen trägt, beispielsweise eine Bilinearform (beispielsweise ein Skalarprodukt bei $K = \mathbb{R}$ oder $K = \mathbb{C}$), so lassen sich weitere wichtige Untergruppen definieren, wie die orthogonale Gruppe $\mathrm{O}(V)$ und die eigentliche Isometriegruppe $\mathrm{SO}(V)$.

Beispiel 3.4. Die symmetrische Gruppe S_n ist die Gruppe der Permutationen auf der Menge $I = \{1, \ldots, n\}$, also

$$S_n = \{\sigma : I \to I \,|\, \sigma \text{ Bijektion}\}$$

mit der Hintereinanderschaltung als Verknüpfung. Das neutrale Element ist die Identität. Eine Permutation wird typischerweise als Wertetabelle geschrieben,

$$\begin{pmatrix} 1 & \ldots & n \\ \sigma(1) & \ldots & \sigma(n) \end{pmatrix}.$$

S_n ist eine Gruppe mit $n!$ Elementen.

Die Permutationsgruppe S_n operiert als Gruppe von linearen Automorphismen auf K^n wie folgt: Der i-te Basisvektor e_i wird auf $e_{\sigma(i)}$ geschickt, also $e_i \mapsto e_{\sigma(i)}$. Dies definiert nach Satz 12.3 (Mathematik (Osnabrück 2009-2011)) einen linearen Automorphismus

$$\sigma\colon\ K^n \longrightarrow K^n,$$

den wir ebenfalls mit σ bezeichnen. In Matrizenschreibweise wird diese lineare Abbildung durch diejenige Matrix beschrieben, bei der in der i-ten Spalte in der $\sigma(i)$-ten Zeile eine 1 steht, und sonst überall 0. Eine solche Matrix nennt man eine Permutationsmatrix. Wenn E_{ij} diejenige Matrix bezeichnet, die genau an der Stelle ij (i-te Zeile, j-te Spalte) eine 1 und sonst überall eine 0 als Eintrag besitzt, so ist die zu σ gehörende Permutationsmatrix gleich

$$E_\sigma = \sum_{i=1}^{n} E_{\sigma(i)i}.$$

Diese Matrix ist in gewissem Sinn der Graph der Permutation.

Die Menge der Permutationsmatrizen bilden eine endliche Untergruppe der allgemeinen linearen Gruppe $\mathrm{GL}_n(K)$, und die Zuordnung $\sigma \mapsto E_\sigma$ ist ein Gruppenisomorphismus zwischen der Permutationsgruppe S_n und dieser endlichen Untergruppe. Nach Beispiel 3.3 operiert die Permutationsgruppe S_n linear auf dem K^n.

Definition 3.5. Es sei K ein Körper und G eine Gruppe, die auf einem K-Vektorraum V linear operiere. Ein Untervektorraum $U \subseteq V$ heißt *G-invariant*, wenn für alle $\sigma \in G$ und alle $v \in U$ auch $\sigma v \in U$ ist.

Dies kann man auch so ausdrücken, dass jede zu $\sigma \in G$ gehörende Abbildung φ_σ den Unterraum U in sich selbst abbildet. D.h. U ist φ_σ-invariant für jedes $\sigma \in G$. Bei endlichdimensionalem V ist dann sogar stets

$$\varphi_\sigma(U) = U.$$

Die Operation lässt sich in natürlicher Weise auf einen jeden invarianten Unterraum einschränken. Man nennt diese Räume daher auch einfach *G-Räume*.

Definition 3.6. Es sei K ein Körper und G eine Gruppe, die auf einem K-Vektorraum V linear operiere. Der Untervektorraum

$$\{v \in V \,|\, \sigma v = v \text{ für alle } \sigma \in G\}$$

heißt der *Fixraum* der Gruppenoperation.

Der Fixraum ist einfach die Menge aller Fixpunkte der Operation. Er ist ein G-invarianter Untervektorraum.

Darstellungstheorie

Eine lineare Operation einer Gruppe auf einem Vektorraum nennt man auch eine Darstellung der Gruppe. In der Darstellungstheorie steht die Frage im Mittelpunkt, auf wie viele (wesentlich verschiedene) Arten eine bestimmte Gruppe auf einem Vektorraum operieren kann. Mit dieser Kenntnis kann man sowohl die Gruppe selbst als auch ihre Operationen besser verstehen.

Definition 3.7. Es sei G eine Gruppe, K ein Körper und V ein (endlichdimensionaler) K-Vektorraum. Einen Gruppenhomomorphismus

$$\rho\colon\ G \longrightarrow \mathrm{GL}(V)$$

nennt man eine (endlichdimensionale) *Darstellung* (über K).

Man spricht auch von einer *linearen Darstellung*. Bei $V = K^r$ spricht man auch von einer *Matrix-Darstellung*. Das Bild der Darstellung ist eine Untergruppe der allgemeinen linearen Gruppe. Die Dimension des Vektorraumes V nennt man auch die *Dimension der Darstellung*.

Eine Darstellung von G in $\mathrm{GL}(V)$ ist das gleiche wie eine Operation von G auf V. Die *Darstellungstheorie* einer gegebenen Gruppe beschäftigt sich mit der Menge aller möglichen Darstellungen zu dieser Gruppe.

Eine Darstellung

$$\rho\colon\ G \longrightarrow \mathrm{GL}(V)$$

einer Gruppe in einen K-Vektorraum V heißt *treu*, wenn ρ injektiv ist.

Man interessiert sich hauptsächlich für die treuen Darstellungen. Wenn eine Darstellung der Gruppe G nicht treu ist, so besitzt sie einen nichttrivialen Kern $H \subseteq G$, und es ergibt sich nach Satz 5.12 (Körper- und Galoistheorie (Osnabrück 2011)) eine treue Darstellung der Restklassengruppe G/H.

Man unterscheide sorgfältig zwischen abstrakten intrinsischen Eigenschaften einer Gruppe und Eigenschaften, die mit ihrer Einbettung in die allgemeine lineare Gruppe zusammenhängen. Die Eigenschaften einer linearen Operation hängen von beiden ab.

Definition 3.8. Es sei G eine endliche Gruppe und K ein Körper. Unter der *regulären Darstellung* von G versteht man den Gruppenhomomorphismus[2]

$$G \longrightarrow \mathrm{GL}\left(K^G\right),\ \sigma \longmapsto \left(e_\tau \mapsto e_{\sigma\tau}\right).$$

Diese Darstellung ist die Verknüpfung des injektiven Gruppenhomomorphismus

$$G \longrightarrow \mathrm{Perm}\,(G),\ \sigma \longmapsto (\tau \mapsto \sigma\tau)\,,$$

der auch im Satz von Cayley auftaucht, mit dem ebenfalls injektiven Gruppenhomomorphismus, der einer Permutation π auf einer Menge I (die im vorliegenden Fall G ist) ihre lineare, durch $e_i \mapsto e_{\pi(i)}$ festgelegte Realisierung zuordnet. Insbesondere ist die reguläre Darstellung treu, und somit gibt es für jede endliche Gruppe überhaupt eine treue Darstellung. Es lässt sich also jede endliche Gruppe als Untergruppe der Gruppe der invertierbaren Matrizen realisieren, und zwar über jedem Körper.

[2]Hierbei wird durch die Zuordnung $\tau \mapsto \sigma\tau$ eine Permutation auf G definiert; diese gibt die zugehörige lineare Abbildung auf der Standardbasis des K^G vor. Unter K^G verstehen wir die Menge der Abbildungen von G nach K, der isomorph zu $K^{\#(G)}$ ist.

Charaktere

Definition 3.9. Es sei G ein Monoid und K ein Körper. Dann heißt ein Monoidhomomorphismus

$$\chi\colon\ G \longrightarrow (K^\times, 1, \cdot)$$

ein *Charakter* von G in K.

Die Menge der Charaktere von G nach K bezeichnen wir mit $\operatorname{Char}(G,K)$. Mit dem *trivialen Charakter* (also der konstanten Abbildung nach 1) und der Verknüpfung

$$(\chi_1 \cdot \chi_2)(g) := \chi_1(g) \cdot \chi_2(g)$$

ist $\operatorname{Char}(G,K)$ selbst ein Monoid, und zwar ein Untermonoid des Abbildungsmonoid von G nach $K^\times$. Da es zu jedem Charakter den inversen Charakter χ^{-1} gibt, der durch

$$\chi^{-1}(g) = (\chi(g))^{-1}$$

definiert ist, bildet $\operatorname{Char}(G,K)$ sogar eine kommutative Gruppe (siehe unten). Ein Charakter einer Gruppe ist nichts anderes als eine eindimensionale Darstellung.

Definition 3.10. Es sei G ein Gruppe und K ein Körper. Dann nennt man die Menge der Charaktere

$$G^\vee := \operatorname{Char}(G,K) = \left\{\chi : G \to K^\times \,|\, \chi \text{ Charakter}\right\}$$

die *Charaktergruppe* von G (in K).

Lemma 3.11. *Sei G eine Gruppe, K ein Körper und $G^\vee = \operatorname{Char}(G,K)$ die Charaktergruppe zu G. Dann gelten folgende Aussagen.*

(1) *$G^\vee$ ist eine kommutative Gruppe.*
(2) *Bei einer direkten Gruppenzerlegung $G = G_1 \times G_2$ ist $(G_1 \times G_2)^\vee = G_1^\vee \times G_2^\vee$.*

Beweis. Siehe Aufgabe 3.9. □

Lemma 3.12. *Es sei G eine endliche kommutative Gruppe mit dem Exponenten m, und es sei K ein Körper, der eine primitive m-te Einheitswurzel besitzt. Dann sind G und $G^\vee$ isomorphe Gruppen.*

Beweis. Nach Lemma 3.11 (2) und Korollar Anhang 4.2 (Körper- und Galoistheorie (Osnabrück 2011)) kann man annehmen, dass $G = \mathbb{Z}/(n)$ eine endliche zyklische Gruppe ist, und dass K eine n-te primitive Einheitswurzel besitzt. Jeder Gruppenhomomorphismus

$$\varphi\colon\ G \longrightarrow K^\times$$

ist durch $\zeta = \varphi(1)$ eindeutig festgelegt, und wegen

$$\zeta^n = (\varphi(1))^n = \varphi(n) = \varphi(0) = 1$$

ist ζ eine n-te Einheitswurzel. Umgekehrt kann man zu jeder n-ten Einheitswurzel ζ durch die Zuordnung $1 \mapsto \zeta$ nach Lemma 4.4 (Körper- und Galoistheorie (Osnabrück 2011)) und Satz 5.10 (Körper- und Galoistheorie (Osnabrück 2011)) einen Gruppenhomomorphismus von $\mathbb{Z}/(n)$ nach $K^\times$ definieren. Die Menge der n-ten Einheitswurzeln ist, da eine primitive Einheitswurzel vorhanden ist, eine zyklische Gruppe der Ordnung n. Also gibt es n solche Homomorphismen. Wenn ζ eine primitive Einheitswurzel ist, dann besitzt der durch $1 \mapsto \zeta$ festgelegte Homomorphismus die Ordnung n und ist damit ein Erzeuger der Charaktergruppe, also $(\mathbb{Z}/(n))^\vee \cong \mathbb{Z}/(n)$. □

Darstellungen der zyklischen Gruppe

Eine endliche zyklische Gruppe $\mathbb{Z}/(r)$ lässt sich auf unterschiedliche Weise als Untergruppe der allgemeinen linearen Gruppe $\mathrm{GL}(V)$ bzw. $\mathrm{GL}_n(K)$ auffassen, wie die folgenden Beispiele zeigen.

Beispiel 3.13. Es sei K ein Körper, der eine r-te primitive Einheitswurzel ζ besitzt. Dann ist die Untergruppe

$$\mu_r(K) := \left\{\zeta^i \mid i = 0, 1, \ldots, r-1\right\} \subseteq K^\times$$

eine zyklische Gruppe der Ordnung r. Somit ist die Zuordnung

$$\mathbb{Z}/(r) \longrightarrow K^\times,\ i \longmapsto \zeta^i,$$

eine (treue) eindimensionale Darstellung (also ein Charakter) einer zyklischen Gruppe.

Beispiel 3.14. Es sei K ein Körper und $G = \mathbb{Z}/(r)$. Der Erzeuger 1 operiert auf $\mathbb{Z}/(r)$ durch Addition mit 1, die zugehörige Permutation ist also durch $k \mapsto k+1$ (und $r \mapsto 1$) gegeben. Die zugehörige Permutationsmatrix ist

$$\begin{pmatrix} 0 & 0 & \ldots & 0 & 1 \\ 1 & 0 & 0 & \ldots & 0 \\ 0 & 1 & 0 & \ldots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \ldots & 0 & 1 & 0 \end{pmatrix}.$$

Somit ist die Zuordnung

$$\mathbb{Z}/(r) \longrightarrow \mathrm{GL}_r(K),\ i \longmapsto \begin{pmatrix} 0 & 0 & \ldots & 0 & 1 \\ 1 & 0 & 0 & \ldots & 0 \\ 0 & 1 & 0 & \ldots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \ldots & 0 & 1 & 0 \end{pmatrix}^i,$$

die reguläre Darstellung der zyklischen Gruppe.

Beispiel 3.15. Es sei K ein Körper und $\zeta_1, \ldots, \zeta_n \in K$ seien Einheitswurzeln. Dann ist

$$\left\{ \begin{pmatrix} \zeta_1^i & 0 & \cdots & \cdots & 0 \\ 0 & \zeta_2^i & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & \zeta_{n-1}^i & 0 \\ 0 & \cdots & \cdots & 0 & \zeta_n^i \end{pmatrix} | \, i = 0, 1, \ldots \right\},$$

eine zyklische Untergruppe der allgemeinen linearen Gruppe $\mathrm{GL}_n(K)$. Ihre Ordnung ist das kleinste gemeinsame Vielfache (nennen wir es r) der Ordnungen der ζ_j. Die Zuordnung

$$\mathbb{Z}/(r) \longrightarrow \mathrm{GL}_n(K), \, i \longmapsto \begin{pmatrix} \zeta_1^i & 0 & \cdots & \cdots & 0 \\ 0 & \zeta_2^i & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & \zeta_{n-1}^i & 0 \\ 0 & \cdots & \cdots & 0 & \zeta_n^i \end{pmatrix},$$

ist eine n-dimensionale Darstellung einer zyklischen Gruppe.

Beispiel 3.16. Es sei K ein Körper, der eine r-te primitive Einheitswurzel ζ besitzt. Dann ist die Untergruppe

$$\left\{ \begin{pmatrix} \zeta^i & 0 \\ 0 & \zeta^{-i} \end{pmatrix} | \, i = 0, 1, \ldots, r-1 \right\},$$

der speziellen linearen Gruppe $\mathrm{SL}_2(K)$ eine zyklische Gruppe der Ordnung r ist. Die Zuordnung

$$\mathbb{Z}/(r) \longrightarrow \mathrm{SL}_2(K), \, i \longmapsto \begin{pmatrix} \zeta^i & 0 \\ 0 & \zeta^{-i} \end{pmatrix},$$

ist eine zweidimensionale Darstellung einer zyklischen Gruppe.

Beispiel 3.17. Eine jede invertierbare Matrix $M \in \mathrm{GL}_n(K)$ endlicher Ordnung über einem Körper K erzeugt eine endliche zyklische Untergruppe der allgemeinen linearen Gruppe. Ihre Determinante muss eine Einheitswurzel sein, deren Ordnung die Ordnung der Matrix teilt. Auch die Eigenwerte einer solchen Matrix müssen Einheitswurzeln sein. Wie das reelle Beispiel $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ zeigt, muss eine Matrix endlicher Ordnung weder diagonalisierbar noch trigonalisierbar sein. Über einem endlichen Körper besitzt jede invertierbare Matrix eine endliche Ordnung.

Beispiel 3.18. Es sei K ein Körper der positiven Charakteristik $p > 0$. Dann bilden die Matrizen

$$\left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} | \, a \in \mathbb{Z}/(p) \right\}$$

eine zyklische Untergruppe der $\mathrm{SL}_2(K)$ mit p Elementen.

Satz 3.19. *Es sei K ein algebraisch abgeschlossener Körper der Charakteristik 0. Dann ist jede invertierbare Matrix $M \in \mathrm{GL}_n(K)$, die endliche Ordnung besitzt, diagonalisierbar.*

Beweis. Die Matrix ist trigonalisierbar und besitzt eine jordansche Normalform. Wir zeigen, dass die einzelnen Jordanblöcke

$$\begin{pmatrix} \lambda & 1 & 0 & \cdots & \cdots & 0 \\ 0 & \lambda & 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & \lambda & 1 & 0 \\ 0 & \cdots & \cdots & 0 & \lambda & 1 \\ 0 & \cdots & \cdots & \cdots & 0 & \lambda \end{pmatrix}$$

trivial sind. Wegen der endlichen Ordnung muss λ eine Einheitswurzel sein. Durch Multiplikation mit $\lambda^{-1}E_n$ können wir davon ausgehen, dass eine Matrix der Form

$$\begin{pmatrix} 1 & a & 0 & \cdots & \cdots & 0 \\ 0 & 1 & a & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 1 & a & 0 \\ 0 & \cdots & \cdots & 0 & 1 & a \\ 0 & \cdots & \cdots & \cdots & 0 & 1 \end{pmatrix}$$

(mit $a \neq 0$) vorliegt. Wenn dies keine 1×1-Matrix ist, so gibt es zwei Vektoren u, v, wobei u ein Eigenvektor ist und v auf $v + au$ abgebildet wird. Die k-te Iteration der Matrix schickt dann v auf $v + kau$ und wegen Charakteristik 0 ist dies nicht v, im Widerspruch zur endlichen Ordnung. □

Korollar 3.20. *Es sei K ein algebraisch abgeschlossener Körper der Charakteristik 0. Dann ist jede Darstellung einer endlichen zyklischen Gruppe $\mathbb{Z}/(r)$ in $\mathrm{GL}_n(K)$ in einer geeigneten Basis von der Form*

$$\mathbb{Z}/(r) \longrightarrow \mathrm{GL}_n(K),\ i \longmapsto \begin{pmatrix} \zeta_1^i & 0 & \cdots & \cdots & 0 \\ 0 & \zeta_2^i & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & \zeta_{n-1}^i & 0 \\ 0 & \cdots & \cdots & 0 & \zeta_n^i \end{pmatrix},$$

mit gewissen Einheitswurzeln ζ_j.

Beweis. Dies folgt unmittelbar aus Satz 3.19. □

3. Arbeitsblatt

Aufwärmaufgaben

Aufgabe 3.1. Überprüfe, dass die reguläre Darstellung in der Tat ein Gruppenhomomorphismus ist. Wie sieht es aus, wenn man die reguläre Darstellung mit der Rechtsmultiplikation statt mit der Linksmultiplikation definiert?

Aufgabe 3.2. Zeige, dass jede endliche Gruppe eine treue Darstellung innerhalb der speziellen linearen Gruppe besitzt.

Aufgabe 3.3. Finde treue Darstellungen für $\mathbb{Z}$.

Aufgabe 3.4. Finde treue Darstellungen für $\mathbb{Q}$.

Aufgabe 3.5. Es sei K ein Körper und $G \subseteq \mathrm{GL}_n(K)$ eine zyklische Untergruppe, die von $\varphi \in \mathrm{GL}_n(K)$ erzeugt werde. Zeige, dass ein Untervektorraum $U \subseteq K^n$ genau dann G-invariant ist, wenn er φ-invariant ist.

Aufgabe 3.6. Es sei $\mathbb{F}_q$ ein endlicher Körper. Bestimme die Anzahl der Elemente in

$$\mathrm{GL}_n(\mathbb{F}_q) .$$

Aufgabe 3.7. Es sei $\mathbb{F}_q$ ein endlicher Körper. Bestimme die Anzahl der Elemente in

$$\mathrm{SL}_n(\mathbb{F}_q) .$$

Aufgabe 3.8. Berechne die Ordnung der Matrix

$$\begin{pmatrix} 2 & 4 & 1 \\ 3 & 2 & 0 \\ 0 & 1 & 3 \end{pmatrix}$$

über dem Körper $\mathbb{F}_5$.

Aufgabe 3.9. Sei G eine Gruppe, K ein Körper und $G^\vee = \mathrm{Char}(G, K)$ die Charaktergruppe zu G. Beweise die folgenden Aussagen.

(1) $G^\vee$ ist eine kommutative Gruppe.

(2) Bei einer direkten Gruppenzerlegung $G = G_1 \times G_2$ ist $(G_1 \times G_2)^\vee = G_1^\vee \times G_2^\vee$.

Aufgabe 3.10.*

Es seien D_1 und D_2 kommutative Gruppen und seien $D_1^\vee$ und $D_2^\vee$ die zugehörigen Charaktergruppen zu einem Körper K.

(1) Zeige, dass zu einem Gruppenhomomorphismus

$$\varphi\colon\ D_1 \longrightarrow D_2$$

durch die Zuordnung $\chi \mapsto \chi \circ \varphi$ ein Gruppenhomomorphismus

$$\varphi^\vee\colon\ D_2^\vee \longrightarrow D_1^\vee$$

definiert wird.

(2) Es sei D_3 eine weitere kommutative Gruppe und sei

$$\psi\colon\ D_2 \longrightarrow D_3$$

ein Gruppenhomomorphismus. Zeige die Gleichheit

$$(\psi \circ \varphi)^\vee\ =\ \varphi^\vee \circ \psi^\vee.$$

Aufgabe 3.11. Es sei D eine kommutative Gruppe und K ein Körper.

a) Zeige, dass durch

$$D \longrightarrow (D^\vee)^\vee,\ d \longmapsto (\mathrm{ev}_d : \chi \mapsto \chi(d)),$$

ein natürlicher Gruppenhomomorphismus von D in das Doppeldual $(D^\vee)^\vee$ gegeben ist.

b) Es sei nun D endlich und es sei vorausgesetzt, dass K eine m-te primitive Einheitswurzel enthält, wobei m der Exponent von D sei. Zeige, dass dann die Abbildung aus a) ein Isomorphismus ist.

Die in der vorstehenden Aufgabe auftretende Abbildung ev_d heißt *Evaluierungsabbildung* (zu d).

Aufgabe 3.12. Es sei D eine endliche kommutative Gruppe und es sei K ein Körper. Wir betrachten die Zuordnung

$$E \longmapsto E^\perp = \{\chi \in D^\vee |\, \chi(d) = 1 \text{ für alle } d \in E\}\ ,$$

die einer Untergruppe von D eine Untergruppe von $D^\vee$ zuordnet. Zeige die folgenden Aussagen.

a) Die Zuordnung ist inklusionsumkehrend.

b) Unter der kanonischen Abbildung

$$D \longrightarrow (D^\vee)^\vee,\ d \longmapsto (\mathrm{ev}_d : \chi \mapsto \chi(d)),$$

ist $\mathrm{ev}_d(E) \subseteq (E^\perp)^\perp$.

c) Es sei vorausgesetzt, dass K eine m-te primitive Einheitswurzel enthält, wobei m der Exponent von D sei. Zeige, dass dann $\mathrm{ev}_d(E) = (E^\perp)^\perp$ gilt.

Aufgabe 3.13. Es sei D eine endliche kommutative Gruppe mit dem Exponenten m, und es sei K ein Körper, der eine primitive m-te Einheitswurzel besitzt. Zeige, dass die Zuordnungen

$$E \longmapsto E^\perp = \{\chi \in D^\vee |\, \chi(d) = 1 \text{ für alle } d \in E\}$$

und

$$H \longmapsto H^\perp = \{d \in D |\, \chi(d) = 1 \text{ für alle } \chi \in H\}$$

(zwischen den Untergruppen von D und den Untergruppen von $D^\vee$) zueinander invers sind.

Aufgabe 3.14. Sei D eine endliche kommutative Gruppe mit der zugehörigen Charaktergruppe $D^\vee$ in einen Körper K. Zeige, dass die Abbildung

$$D^\vee \longrightarrow K^\times,\ \chi \longmapsto \prod_{d \in D} \chi(d),$$

ein Gruppenhomomorphismus ist.

Aufgaben zum Abgeben

Aufgabe 3.15. (4 Punkte)

Man gebe ein Beispiel einer Untergruppe $G \subseteq \mathrm{GL}_r(K)$ mit $r \geq 2$, die von zwei Elementen erzeugt wird, die beide als Endomorphismen diagonalisierbar sind, derart, dass die einzigen G-invarianten Untervektorräume 0 und K^r sind.

Aufgabe 3.16. (4 Punkte)

Wir betrachten die natürliche Operation der Permutationsgruppe $G = S_n$ auf K^n.

a) Bestimme den Fixraum F der Operation.

b) Finde ein G-invariantes Komplement, also einen G-invarianten Unterraum $U \subseteq K^n$ mit $F \oplus U = K^n$.

Aufgabe 3.17. (5 Punkte)

Betrachte die Untergruppe

$$G \subset \mathrm{Gl}\,(2,\mathbb{R})\,,$$

die durch die drei Matrizen

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

erzeugt wird. Liste die Elemente dieser Gruppe auf und bestimme sämtliche Untergruppen.

Aufgabe 3.18. (4 Punkte)

Es sei K ein Körper und sei D eine endliche kommutative Gruppe mit dem Exponenten m. Zeige, dass folgende Aussagen äquivalent sind.

(1) K besitzt eine m-te primitive Einheitswurzel.
(2) Zu jedem Primpotenzteiler p^r von m besitzt K eine p^r-te primitive Einheitswurzel.
(3) Zu jedem Teiler n von m besitzt K eine n-te primitive Einheitswurzel.
(4) Zu jeder Ordnung n eines Elementes $d \in D$ besitzt K eine n-te primitive Einheitswurzel.

Aufgabe 3.19. (4 (1+3) Punkte)

Es sei D eine endliche kommutative Gruppe und $E \subseteq D$ eine Untergruppe. Es sei K ein Körper.

a) Zeige, dass der Kern des natürlichen Gruppenhomomorphismus

$$\psi\colon\ D^\vee \longrightarrow E^\vee,\ \chi \longmapsto \chi|_E,$$

gleich $E^\perp$ ist.

b) Es sei vorausgesetzt, dass K eine m-te primitive Einheitswurzel besitzt, wobei m der Exponent von D sei. Zeige, dass ψ surjektiv ist.

4. Vorlesung - Invariantenringe I

Induzierte Darstellungen

Proposition 4.1. *Es sei K ein Körper, V ein K-Vektorraum und*

$$G \times V \longrightarrow V$$

eine lineare Operation einer Gruppe G auf V. Durch diese Operation werden folgende lineare Operationen induziert.

(1) *Die Operation auf dem k-ten Produkt*[3] *von V mit sich selbst, also*

$$G \times V^k \longrightarrow V^k,\ (\sigma, v_1, \ldots, v_k) \longmapsto (\sigma(v_1), \ldots, \sigma(v_k)).$$

(2) *Die Operation auf dem k-ten Dachprodukt $\bigwedge^k V$, also*

$$G \times \bigwedge^k V \longrightarrow \bigwedge^k V,$$

die durch $v_1 \wedge \ldots \wedge v_k \mapsto \sigma(v_1) \wedge \ldots \wedge \sigma(v_k)$ festgelegt ist.

(3) *Die duale Operation (von rechts) auf dem Dualraum V^*, also die Abbildung*

$$V^* \times G \longrightarrow V^*,\ (f, \sigma) \longmapsto f \circ \sigma.$$

Beweis. Siehe Aufgabe 4.1. □

Lineare Operationen und der Polynomring

Es sei G eine Gruppe, die auf einer Menge X (beispielsweise einem Vektorraum) operiere. Es sei K ein Körper und

$$f\colon X \longrightarrow K$$

eine beliebige Funktion mit X als Definitionsbereich und K als Zielbereich. Die Menge dieser Funktionen bilden einen kommutativen Ring, wobei je zwei Funktionen addiert oder multipliziert werden, indem an jedem Punkt $x \in X$ die Werte dieser Funktion addiert bzw. multipliziert werden. Zu $\sigma \in G$, aufgefasst als Bijektion

$$\sigma\colon X \longrightarrow X,$$

ergibt sich die neue Funktion

$$X \xrightarrow{\sigma} X \xrightarrow{f} K\,,$$

also $f \circ \sigma$. Die Gruppe operiert also auch auf dem Funktionenring, und zwar wegen

$$f \circ (\sigma\tau) = (f \circ \sigma) \circ \tau$$

von rechts. Zu diesem Übergang vergleiche auch Beispiel 2.25.

Auf einem K-Vektorraum sind die einfachsten Funktionen von V nach K die Linearformen. Wenn eine Gruppe G linear auf V operiert, so ist die Zuordnung (vergleiche Proposition 4.1)

$$V^* \times G \longrightarrow V^*,\ (f, \sigma) \longmapsto f \circ \sigma,$$

selbst K-linear.

Bei $V = K^n$ bilden die Projektionen p_i, wobei die Projektion p_i ein Tupel $(x_1, \ldots, x_n)$ auf seine i-te Komponente x_i abbildet, eine Basis von V^* (die sogenannte *Dualbasis*). Ein Polynom $f \in K[X_1, \ldots, X_n]$ aus dem Polynomring in n Variablen über K kann man direkt als eine Funktion (die zugehörige

[3] Diese Konstruktion lag schon Beispiel 1.1 zugrunde.

Polynomfunktion) von K^n nach K interpretieren, indem man in das Polynom das Tupel $(x_1, \ldots, x_n)$ einsetzt, bzw. die Variable X_i als die i-te Projektion p_i interpretiert.

Man möchte nun jedem endlichdimensionalen K-Vektorraum V einen Polynomring $K[V]$ zuordnen, dessen Elemente man als K-wertige Funktionen auf V auffassen kann. Da es stets eine lineare Isomorphie $V \cong K^n$ gibt, wird es auch einen K-Algebraisomorphismus $K[V] \cong K[X_1, \ldots, X_n]$ geben.

Definition 4.2. Es sei K ein endlichdimensionaler K-Vektorraum. Man nennt die von allen formalen Monomen $f_1 \cdot f_2 \cdots f_m$, wobei die f_i Linearformen auf V sind, symbolisch erzeugte kommutative K-Algebra, die die linearen Beziehungen zwischen den Linearformen respektiert, den *Polynomring* zu V. Er wird mit

$$K[V]$$

bezeichnet.

Bemerkung 4.3. Jedes Element in $K[V]$ besitzt eine Darstellung der Form

$$\sum_{\nu} a_\nu f_\nu$$

(mit endlicher Indexmenge), wobei $a_\nu \in K$ und f_ν ein formales Produkt aus Linearformen ist. In einem solchen Produkt sind wegen der geforderten Kommutativität die Faktoren vertauschbar. Da lineare Relationen zwischen den Linearformen respektiert werden müssen, folgt aus einer Gleichung

$$g = b_1 g_1 + \ldots + b_\ell g_\ell$$

für Linearformen $g, g_1, \ldots, g_\ell$ die Gleichung

$$g f_2 \cdots f_m = \sum_{j=1}^{\ell} b_j g_j f_2 \cdots f_m.$$

Wenn V n-dimensional ist und $f_1, \ldots, f_n$ eine Basis von V^* ist, so lässt sich daher jedes Element aus $K[V]$ als Polynom in den f_i schreiben. Diese Darstellung ist auch eindeutig, da es in $K[V]$ nur Relationen gibt, die von einer linearen Relation herrühren, es solche aber in einer Basis nicht gibt. D.h. es gibt einen K-Algebraisomorphismus

$$K[X_1, \ldots, X_n] \longrightarrow K[V],\ X_i \longmapsto f_i.$$

Bemerkung 4.4. Es sei K ein unendlicher Körper und V ein endlichdimensionaler K-Vektorraum. Dann lässt sich der Polynomring $K[V]$ auch als die von sämtlichen Linearformen erzeugte K-Unteralgebra von Abb (V, K) definieren. Dies beruht darauf, dass ein Polynom $\neq 0$ auf K^n (also als Polynomfunktion aufgefasst) nicht die Nullfunktion ist. Bei einem endlichen Körper ist dies nicht richtig, wie das Polynom $X^p - X$ über $\mathbb{Z}/(p)$ zeigt.

Definition 4.5. Es sei K ein Körper, V, W seien endlichdimensionale K-Vektorräume und $\varphi\colon V \to W$ sei eine lineare Abbildung. Den durch

$$\varphi^*\colon W^* \longrightarrow V^*$$

über $f_1 \cdots f_m \mapsto \varphi^*(f_1) \ldots \varphi^*(f_m)$ gegebenen K-Algebrahomomorphismus

$$K[W] \longrightarrow K[V]$$

nennt man *induzierten Algebrahomomorphismus*.

Bemerkung 4.6. Es sei

$$\varphi\colon K^n \longrightarrow K^m$$

eine lineare Abbildung, die durch eine $m \times n$-Matrix A gegeben sei. Dann wird der zugehörige K-Algebrahomomorphismus

$$K[Y_1, \ldots, Y_m] \longrightarrow K[X_1, \ldots, X_n]$$

durch $Y_j \mapsto \sum_{k=1}^n a_{jk} X_k$ gegeben. Nach Definition wird Y_j auf die Hintereinanderschaltung

$$K^n \xrightarrow{\varphi} K^m \xrightarrow{p_j} K$$

abgebildet. Diese schickt den i-ten Standardvektor e_i auf

$$p_j\left(\varphi(e_i)\right) \;=\; p_j\left(\sum_{k=1}^m a_{ki} e_k\right) \;=\; a_{ji}.$$

Durch diese Bedingungen ist aber gerade

$$\sum_{k=1}^n a_{jk} p_k \;=\; \sum_{k=1}^n a_{jk} X_k$$

charakterisiert. Zu einer Linearform $\sum_{j=1}^m b_j Y_j$ berechnet man also das Bild $\sum_{i=1}^n c_i X_i$, indem man $c = A^{tr} b$ ausrechnet. Für ein beliebiges Polynom $F \in K[Y_1, \ldots, Y_m]$ ergibt sich ds Bild, indem man in F jedes Y_j durch den angegebenen Ausdruck ersetzt.

Definition 4.7. Es sei K ein Körper, V ein endlichdimensionaler K-Vektorraum und

$$G \times V \longrightarrow V$$

eine lineare Operation einer Gruppe G auf V. Es sei $K[V]$ der Polynomring zu V. Die Operation der Gruppe G (von rechts) auf $K[V]$, die für jedes $\sigma \in G$ per Definition 4.5 durch die Zuordnung

$$V^* \longrightarrow V^*,\; f \longmapsto f \circ \sigma,$$

festgelegt ist, nennt man die *induzierte Operation auf dem Polynomring*.

Beispiel 4.8. Es sei K ein Körper. Wir betrachten die symmetrische Gruppe S_n, die auf K^n linear operiert, indem $\sigma \in S_n$ den i-ten Standardvektor e_i auf $e_{\sigma(i)}$ schickt (wie in Beispiel 3.4). Diese Gruppenoperation induziert gemäß Definition 4.7 eine Operation auf dem Polynomring $K[X_1, \ldots, X_n]$. Dabei wird X_i auf $X_{\sigma^{-1}(i)}$ geschickt! Abgesehen von diesem Invertieren ist diese

Operation der S_n auf dem Polynomring nichts anderes als die in der ersten Vorlesung besprochene Operation.

Wenn eine Gruppe auf dem K^n durch Diagonalmatrizen operiert, wie in Beispiel 3.15 und Ähnlichen, so erübrigt sich das Transponieren, wenn man zur zugehörigen Operation auf dem Polynomring übergeht.

Beispiel 4.9. Auf einem K-Vektorraum V operiert die Einheitengruppe $K^\times$ durch skalare Multiplikation. Die entsprechende Operation auf dem Polynomring $K[V]$ ist für $\lambda \in K^\times$ durch $f \mapsto \lambda f$ für eine Linearform f gegeben. Ein Produkt $f_1 \cdots f_d$ von Linearformen wird auf $\lambda^d f_1 \cdots f_d$ abgebildet.

Beispiel 4.10. Es sei K ein Körper, der eine r-te primitive Einheitswurzel ζ besitzt. Wir betrachten die in Beispiel 3.13 beschriebene Operation von

$$\mathbb{Z}/(r) \cong \mu_r(K)$$

auf K durch skalare Multiplikation. Die zugehörige Operation auf dem Polynomring $K[X]$ ist dadurch gegeben, dass $\zeta^i \in \mu_r(K)$ durch $X \mapsto \zeta^i X$ wirkt. Somit wird eine Potenz X^j auf $\zeta^{ij} X^j$ abgebildet. Insbesondere ist das Polynom X^r fix unter dieser Gruppenoperation.

Zu einem Vektorraum V ist der Polynomring $K[V]$ in natürlicher Weise[4] $\mathbb{N}$-graduiert, und zwar besteht die d-te Stufe aus Linearkombinationen von Produkten der Form $f_1 \cdots f_d$, wobei die f_j Linearformen sind.

Lemma 4.11. *Es sei K ein Körper, V ein endlichdimensionaler K-Vektorraum und*

$$G \times V \longrightarrow V$$

eine lineare Operation einer Gruppe G auf V. Dann ist die induzierte Operation auf dem Polynomring $R = K[V]$ homogen, d.h. für jedes $\sigma \in G$ und $f \in R_d$ ist auch $f\sigma \in R_d$.

Beweis. Siehe Aufgabe 4.2. □

Die Stufen R_d sind also G-invariante Untervektorräume von R.

Invariantenringe

Da eine Operation einer Gruppe von links auf einem geometrischen Objekt in natürlicher Weise zu einer Operation von rechts auf dem Ring der Funktionen führt, werden wir im Folgenden die Operationen auf einem Ring generell von rechts schreiben.

[4]Die Formulierung „in natürlicher Weise“ kann man an dieser Stelle gut erläutern. Die angesprochene $\mathbb{N}$-Graduierung von $K[V]$ besteht unabhängig und ohne Bezug auf eine Basis. Man kann einen Polynomring auch mit einer $\mathbb{Z}^n$-Graduierung versehen, doch ist dies abhängig von einer gewählten Basis.

Definition 4.12. Es sei G eine Gruppe, die auf einem kommutativen Ring R als Gruppe von Ringautomorphismen operiert (von rechts). Dann bezeichnet man

$$R^G = \{f \in R | \, f\sigma = f \text{ für alle } \sigma \in G\}$$

als den *Invariantenring* (oder *Fixring*) von R unter der Operation von G.

Das ist in der Tat wieder ein Ring, ein Unterring von R. Die 0 und die 1 sind invariant, da alle $\sigma \in G$ als Ringautomorphismen operieren. Ebenso ist mit invarianten Funktionen $f, g \in R^G$ auch das Negative $-f$, deren Summe $f+g$ und deren Produkt fg invariant.

Bemerkung 4.13. Es sei R eine kommutative K-Algebra über einem Körper und es sei G eine Gruppe, die als Gruppe von K-Algebraautomorphismen operiere. Zu jedem $\sigma \in G$ sei also

$$\sigma \colon R \longrightarrow R$$

ein K-Algebrahomomorphismus. Dann ist $K \subseteq R^G$ und der Fixring R^G ist selbst eine K-Algebra. Zu einer linearen Operation von G auf einem K-Vektorraum V ist die zugehörige Operation von G auf dem Polynomring $K[V]$ eine Operation als Gruppe von K-Automorphismen.

Lemma 4.14. *Es sei G eine Gruppe, die auf einem kommutativen Ring R als Gruppe von Ringautomorphismen operiere. Dann gelten folgende Aussagen.*

(1) *Für die Einheiten gilt*

$$\left(R^G\right)^\times = R^G \cap R^\times.$$

(2) *Wenn R ein Körper ist, so ist auch R^G ein Körper.*

Beweis. Siehe Aufgabe 4.4. □

Lemma 4.15. *Es sei K ein Körper, V ein endlichdimensionaler K-Vektorraum und*

$$G \times V \longrightarrow V$$

eine lineare Operation einer Gruppe G auf V. Dann ist der Fixring $R^G \subseteq R = K[V]$ der induzierten Operation auf dem Polynomring $K[V]$ ein $\mathbb{N}$-graduierter Unterring. Dabei ist

$$\left(R^G\right)_d = (R_d)^G,$$

die d-te Stufe des Fixringes ist der Fixraum der induzierten Operation auf der d-ten Stufe des Polynomringes.

Beweis. Dies folgt unmittelbar aus Lemma 4.1. □

In diesem Fall ist also die Bestimmung des Fixringes gleichbedeutend mit der Bestimmung des Fixraumes zu $K[V]_d$ für jedes $d \in \mathbb{N}$.

Beispiel 4.16. Es sei K ein Körper, der eine r-te primitive Einheitswurzel ζ besitzt. Wir betrachten die Operation von $\mu_r(K)$ auf K und auf $K[X]$ durch skalare Multiplikation (siehe Beispiel 3.13 und Beispiel 4.10). Der Fixring zu dieser Operation ist $K[X^r]$. Dazu muss man nur die Wirkungsweise des Erzeugers ζ der Gruppe verstehen und nach Lemma 4.15 muss man nur die (eindimensionalen) homogenen Stufen $K[X]_d = K \cdot X^d$ betrachten. Die induzierte Operation ist $X^d \mapsto \zeta^d X^d$. Dies ist genau dann die Identität, wenn d ein Vielfaches von r ist. Daher bilden die Stufen $K[X]_{md}$ den Invariantenring.

Beispiel 4.17. Zur natürlichen Operation der symmetrischen Gruppe S_n auf K^n bzw. auf $K[X_1, \ldots, X_n]$ ist der Fixring

$$K[X_1, \ldots, X_n]^{S_n} = K[E_1, \ldots, E_n],$$

wobei die E_i die elementarsymmetrischen Polynome sind. Dies ist die Existenzaussage von Satz 1.7; die dortige Eindeutigkeitsaussage bedeutet, dass der Fixring isomorph zu einem Polynomring in n Variablen ist.

Bemerkung 4.18. Die Elemente eines Polynomrings $K[V]$ zu einem K-Vektorraum V kann man als Funktionen von V nach K auffassen. Wenn eine lineare Operation einer Gruppe G auf V vorliegt, so ist ein Element $f \in K[V]^G \subseteq K[V]$ eine invariante Funktion von V nach K im Sinne von Definition 2.21. Zu $\sigma \in G$ und $v \in V$ ist ja

$$f(\sigma(v)) = (f\sigma)(v) = f(v).$$

Wenn K unendlich ist, so gilt hiervon auch die Umkehrung, d.h. ein Polynom $f \in K[V]$, das aufgefasst als Funktion auf V invariant ist, gehört zum Invariantenring $K[V]^G$, siehe Aufgabe 4.13. Bei endlichem K muss die Umkehrung nicht gelten, siehe Beispiel 4.19. Wir werden später sehen, dass es zu jedem kommutativen Ring einen topologischen Raum gibt, auf dem man Elemente des Invariantenringes zu einer Gruppenoperation als invariante Abbildungen auffassen kann.

Beispiel 4.19. Wir betrachten die natürliche Operation der symmetrischen Gruppe $G = S_2 \cong \mathbb{Z}/(2)$ auf $V = (\mathbb{Z}/(p))^2$ ($p \geq 3$), das nichttriviale Element vertauscht die Komponenten (das entspricht der Matrix $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$bzw.) $X \longleftrightarrow Y$. Wegen

$$f = XY^p - X^pY = X(Y^p - Y) - Y(X^p - X)$$

ist dieses Polynom, aufgefasst als Funktion auf V, die Nullfunktion und somit insbesondere G-invariant. Dagegen ist f kein symmetrisches Polynom und gehört nicht zu $\mathbb{Z}/(p)[X, Y]^G$.

4. Arbeitsblatt

Aufwärmaufgaben

Aufgabe 4.1. Es sei K ein Körper, V ein K-Vektorraum und

$$G \times V \longrightarrow V$$

eine lineare Operation einer Gruppe G auf V. Zeige, dass dadurch in natürlicher Weise die folgenden linearen Operationen induziert sind.

(1) Die Operation auf dem k-ten Produkt von V mit sich selbst, also

$$G \times V^k \longrightarrow V^k,\ (\sigma, v_1, \ldots, v_k) \longmapsto (\sigma(v_1), \ldots, \sigma(v_k)).$$

(2) Die Operation auf dem k-ten Dachprodukt $\bigwedge^k V$, also

$$G \times \bigwedge^k V \longrightarrow \bigwedge^k V,$$

die durch $v_1 \wedge \ldots \wedge v_k \mapsto \sigma(v_1) \wedge \ldots \wedge \sigma(v_k)$ festgelegt ist.

(3) Die duale Operation (von rechts) auf dem Dualraum V^*, also die Abbildung

$$V^* \times G \longrightarrow V^*,\ (f, \sigma) \longmapsto f \circ \sigma.$$

Aufgabe 4.2. Es sei K ein Körper, V ein endlichdimensionaler K-Vektorraum und

$$G \times V \longrightarrow V$$

eine lineare Operation einer Gruppe G auf V. Zeige, dass die induzierte Operation auf dem Polynomring $K[V]$ homogen, d.h. dass für jedes $\sigma \in G$ und $f \in R_d$ auch $f\sigma \in R_d$ gilt.

Aufgabe 4.3. Bestimme in Beispiel 3.15 und Beispiel 3.18 die induzierte Wirkung der Gruppe auf der d-ten Stufe des Polynomringes $K[V]$.

Aufgabe 4.4. Es sei G eine Gruppe, die auf einem kommutativen Ring R als Gruppe von Ringautomorphismen operiere. Zeige die folgende Aussagen.

(1) Für die Einheiten gilt

$$\left(R^G\right)^\times = R^G \cap R^\times.$$

(2) Wenn R ein Körper ist, so ist auch R^G ein Körper.

Aufgabe 4.5. Es sei G eine endliche Gruppe, die auf einem kommutativen Ring R als Gruppe von Ringautomorphismen operiere. Zeige, dass zu jedem $f \in R$ sowohl $\sum_{\sigma \in G} f\sigma$ als auch $\prod_{\sigma \in G} f\sigma$ zum Fixring R^G gehören.

Aufgabe 4.6. Es sei K ein unendlicher Körper und $K[X_1, \ldots, X_n]$ der Polynomring über K. Die Einheitengruppe $K^\times$ operiere durch skalare Multiplikation auf R, d.h. zu $\lambda \in K^\times$ gehört der durch $X_i \mapsto \lambda X_i$ definierte K-Algebraautomorphismus. Zeige, dass der Fixring zu dieser Operation K ist.

Aufgabe 4.7. Betrachte die Operation der symmetrischen Gruppe S_n auf dem Polynomring $R = K[X_1, \ldots, X_n]$ über einem Körper K. Bestimme (zu $n = 2, 3, 4$) für jede Untergruppe $H \subseteq S_n$ den Fixring R^H.

Aufgabe 4.8. Es sei S ein kommutativer Ring mit $2 \neq 0$ und $a \in S$. Zeige, dass die Gruppe $\mathbb{Z}/(2) \cong \{1, -1\}$ auf der quadratischen Erweiterung

$$R := S[X]/(X^2 - a)$$

als Gruppe von S-Algebrahomomorphismen operiert, indem -1 durch $X \mapsto -X$ wirkt. Bestimme den Fixring zu dieser Operation.

Aufgabe 4.9. Es sei R ein kommutativer Ring und G eine Gruppe, die auf R als Gruppe von Ringautomorphismen operiere. Zeige, dass die Operation genau dann trivial ist, wenn $R^G = R$ ist.

Aufgabe 4.10. Es sei K ein Körper. Zeige, dass auf $K[X, Y]/(XY)$ eine Gruppenoperation von $\mathbb{Z}/(2)$ gegeben ist, indem das nichttriviale Gruppenelement X und Y vertauscht. Bestimme den Fixring zu dieser Operation.

Aufgabe 4.11. Es sei R ein kommutativer Ring und $G = (R, +)$ die additive Gruppe zu R.

a) Zeige, dass durch die Zuordnung

$$G \longrightarrow \mathrm{Hom}_R^{\mathrm{alg}}\left(R[X], R[X]\right), \; r \longmapsto \varphi_r,$$

wobei φ_r den durch $X \mapsto X + r$ gegebenen R-Algebrahomomorphismus bezeichnet, eine Gruppenoperation von G auf dem Polynomring $R[X]$ definiert ist.

b) Zeige, dass der Fixring zu dieser Operation gleich R ist.

Aufgabe 4.12. Es sei R ein kommutativer Ring und $G = (R^\times, \cdot)$ die multiplikative Gruppe zu R.

a) Zeige, dass durch die Zuordnung

$$G \longrightarrow \mathrm{Hom}_R^{\mathrm{alg}}\left(R[X], R[X]\right), \, r \longmapsto \psi_r,$$

wobei ψ_r den durch $X \mapsto rX$ gegebenen R-Algebrahomomorphismus bezeichnet, eine Gruppenoperation von G auf dem Polynomring $R[X]$ definiert ist.

b) Man gebe Beispiele für kommutative Ringe derart, dass der Fixring zu dieser Operation gleich R ist.

c) Man gebe Beispiele für kommutative Ringe derart, dass der Fixring zu dieser Operation nicht gleich R ist.

Aufgabe 4.13. Es sei K ein unendlicher Körper und V ein K-Vektorraum, auf dem eine Gruppe linear operiere. Zeige, dass $f \in K[V]$ genau dann zu $K[V]^G$ gehört, wenn $f\colon V \to K$ G-invariant ist.

Aufgaben zum Abgeben

Aufgabe 4.14. (4 Punkte)

Wir betrachten die Operation der r-ten komplexen Einheitswurzeln $G = \mu_r(\mathbb{C})$ auf $\mathbb{C}$ durch Multiplikation und die zugehörige Operation auf dem Polynomring $\mathbb{C}[X]$, dessen Fixring $\mathbb{C}[X^r]$ ist. Ferner betrachten wir die reelle Entsprechung dieser Situation, also die Operation auf $\mathbb{R}^2$ durch die Gruppe der Drehmatrizen der Ordnung r und die zugehörige Operation auf $\mathbb{R}[X,Y]$.

a) Zeige

$$\mathbb{R}[\mathrm{Re}\,(z^r)\,,\,\mathrm{Im}\,(z^r)] \subseteq \mathbb{R}[X,Y]^G.$$

b) Zeige, dass diese Inklusion echt sein kann.

Aufgabe 4.15. (6 Punkte)

Betrachte die Untergruppe

$$G \subset \mathrm{GL}_2(\mathbb{R})$$

aus Aufgabe 3.17. Bestimme zu jeder Untergruppe $H \subseteq G$ ein Polynom aus $\mathbb{R}[X,Y]$, das bezüglich H invariant ist, aber nicht bezüglich einer größeren Untergruppe.

Aufgabe 4.16. (6 Punkte)

Es sei K ein Körper der positiven Charakteristik p. Wir betrachten die durch $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ erzeugte zyklische Gruppe und ihre natürliche Operation auf $K[X,Y]$. Zeige, dass der Invariantenring gleich

$$K[Y, X^p - XY^{p-1}]$$

ist.

Aufgabe 4.17. (5 Punkte)

Es sei A ein kommutativer Ring und

$$R = A \times A \times \cdots \times A$$

der n-fache Produktring von A mit sich selbst.

a) Zeige, dass die symmetrische Gruppe S_n auf R durch Vertauschen der Komponenten operiert.

b) Bestimme den Fixring zu dieser Operation.

c) Zeige, dass für jede transitive Untergruppe $H \subseteq S_n$ der Fixring gleich dem Fixring aus Teil (b) ist.

Aufgabe 4.18. (3 Punkte)

Es sei G eine Gruppe, die auf einem kommutativen lokalen Ring als Gruppe von Ringautomorphismen operiere. Zeige, dass der Fixring R^G ebenfalls lokal ist.

5. Vorlesung - Invariantenringe II

Invariantenringe zu Untergruppen

Proposition 5.1. *Es sei $R \times G \to R$ eine Operation einer Gruppe G auf einem kommutativen Ring durch Ringautomorphismen. Sei $H \subseteq G$ eine Untergruppe. Dann gelten folgende Aussagen.*

(1) $R^G \subseteq R^H$.
(2) *Sind H_1 und H_2 Untergruppen in G mit $G = H_1 \cdot H_2$, so ist*
$$R^{H_1} \cap R^{H_2} = R^G .$$
(3) *Ist H ein Normalteiler in G, so operiert die Restklassengruppe G/H auf R^H durch*
$$f[\sigma] := f\sigma .$$
Dabei ist
$$R^G = \left(R^H\right)^{G/H} .$$

Beweis. (1) ist klar. (2). Die Voraussetzung bedeutet, dass man $\sigma = \prod_{i=1}^{n} \sigma_i$ mit gewissen $\sigma_i \in H_1$ oder $\sigma_i \in H_2$ schreiben kann.

Die Inklusion $\supseteq$ ist nach (1) klar. Die Inklusion $\subseteq$ ist wegen

$$f\sigma = f\prod_{i=1}^{n}\sigma_i = f\sigma_1\prod_{i=2}^{n}\sigma_i = f\prod_{i=2}^{n}\sigma_i = f$$

klar. (3). Die Operation ist zunächst wohldefiniert, d.h. unabhängig vom Repräsentanten. Seien dazu $\sigma, \sigma' \in G$ gegeben mit $\sigma'\sigma^{-1} \in H$. Dann ist

$$f\sigma' = f\sigma'\sigma^{-1}\sigma = f\sigma.$$

Wegen der Normalteilereigenschaft gibt es für $\sigma \in G$ und $\tau \in H$ ein $\tau' \in H$ mit $\sigma\tau = \tau'\sigma$. Für $f \in R^H$ ist

$$(f\sigma)\tau = f\tau'\sigma = f\sigma$$

und somit gehört $f\sigma$ ebenfalls zu R^H. Wir haben also eine Abbildung

$$R^H \times G \longrightarrow R^H.$$

Diese Abbildung ist in der Tat eine Gruppenoperation. Das neutrale Element wirkt identisch und die Assoziativität ergibt sich aus

$$f([\sigma][\tau]) = f[\sigma\tau] = f(\sigma\tau) = (f\sigma)\tau = (f[\sigma])\tau = (f[\sigma])[\tau].$$

Es liegt also eine Operation von G auf R^H vor, und da die Elemente $\sigma \in H$ identisch wirken, induziert dies eine Operation von G/H auf R^H. Bei den Abbildungen $f \mapsto f\sigma$ handelt es sich um Ringautomorphismen, da es sich um Einschränkungen von Ringautomorphismen auf R handelt, wobei sich die Surjektivität aus der Existenz von σ^{-1} ergibt.

Wir kommen zur Gleichheit

$$R^G = \left(R^H\right)^{G/H}.$$

Zum Beweis der Inklusion $\subseteq$ sei $f \in R^G$. Dann ist insbesondere $f \in R^H$. Wegen $f[\sigma] = f\sigma = f$ ist f auch G/H- invariant. Zum Beweis der Inklusion $\supseteq$ sei $f \in \left(R^H\right)^{G/H} \subseteq R^H$. Doch dann ist für $\sigma \in G$ wiederum $f\sigma = f[\sigma] = f$. □

Lemma 5.2. *Es sei*

$$R \times G \longrightarrow R$$

eine Operation einer Gruppe G auf einem kommutativen Ring R durch Ringautomorphismen. Es seien $H, H' \subseteq G$ konjugierte Untergruppen. Dann sind die Invariantenringe R^H und $R^{H'}$ in natürlicher Weise isomorph.

Beweis. Die beiden Untergruppen seien vermöge $\tau \in G$ zueinander konjugiert, d.h. die Abbildung

$$H \longrightarrow H',\ \sigma \longmapsto \tau^{-1}\sigma\tau,$$

sei ein Gruppenisomorphismus. Wir betrachten den zu τ gehörenden Ringautomorphismus

$$R \longrightarrow R,\ f \longmapsto f\tau,$$

und seine Einschränkung auf $R^G \subseteq R$. Für $f \in R^H$ und $\sigma' \in H'$ mit $\sigma' = \tau^{-1}\sigma\tau$ ist

$$(f\tau)\sigma' = (f\tau)(\tau^{-1}\sigma\tau) = f\sigma\tau = f\tau,$$

also liegt das Bild in $R^{H'}$. Da man die Rollen von H und H' vertauschen kann, liegt ein Isomorphismus vor. □

Polynomiale Dreiecksinvarianten

Beispiel 5.3. Wir betrachten die Menge der Dreiecke, aufgefasst mit der Operation der Kongruenzabbildungen, siehe Beispiel 1.1. Die Vektoren $v \in \mathbb{R}^2$ fasst man als Verschiebungen T_v und damit als Kongruenzabbildungen auf. Mit einer beliebigen Kongruenz φ besteht die Beziehung $\varphi \circ T_v = T_{\varphi(v)} \circ \varphi$. Daher bilden die Verschiebungen einen Normalteiler in der Kongruenzgruppe G (der uneigentlichen affinen Isometriegruppe). Nach Proposition 5.1 kann man den Invariantenring $\mathbb{R}[X_1, Y_1, X_2, Y_2, X_3, Y_3]^G$ sukzessive berechnen. Unter der Untergruppe V der Verschiebungen ist der Invariantenring offenbar gleich

$$\mathbb{R}[X_1, Y_1, X_2, Y_2, X_3, Y_3]^V = \mathbb{R}[X_1 - X_3, Y_1 - Y_3, X_2 - X_3, Y_2 - Y_3].$$

Dieser Übergang entspricht geometrisch der Verschiebung des dritten Eckpunktes in den Nullpunkt. Die Operation der Restklassengruppe, die ja die uneigentliche Drehgruppe ist, auf diesem Polynomring in vier Variablen (die wir jetzt U_1, V_1, U_2, V_2 nennen) rührt von der natürlichen (und linearen) Operation der Drehgruppe auf dem $\mathbb{R}^2$ her. Die Determinante induziert einen surjektiven Gruppenhomomorphismus

$$\mathrm{O}_2(\mathbb{R}) \longrightarrow \{1, -1\},$$

deren Kern die eigentliche Drehgruppe $\mathrm{SO}_2(\mathbb{R})$ ist (das Urbild von -1 bilden die *Drehspiegelungen*). Daher gibt es eine natürliche Operation der $\mathbb{Z}/(2)$ auf

$$\mathbb{R}[U_1, V_1, U_2, V_2]^{\mathrm{SO}_2(\mathbb{R})},$$

und man sollte zuerst diesen Invariantenring ausrechnen. Aufgrund der geometrischen Interpretation (die drei Quadrate der Längen des Dreiecks, das Skalarprodukt der Seiten am Nullpunkt, der orientierte Flächeninhalt (bis auf Skalierung)) müssen

$$U_1^2 + V_1^2,\ U_2^2 + V_2^2,\ (U_1 - U_2)^2 + (V_1 - V_2)^2,\ U_1U_2 + V_1V_2,\ U_1V_2 - U_2V_1$$

invariante Polynome sein, was man auch direkt durch Rechnungen bestätigen kann. Das Skalarprodukt ist dabei unmittelbar mit den ersten drei Längenquadraten polynomial ausdrückbar. Da die drei Längen zwar die unorientierte Kongruenzklasse des Dreiecks bestimmen, es zu einem (nicht entarteten) Längentripel aber zwei entgegengesetzt orientierte Dreiecke gibt, muss es ein

weiteres $\mathrm{SO}_2(\mathbb{R})$-invariantes Polynom geben, das aber nicht $\mathrm{O}_2(\mathbb{R})$-invariant ist, sondern Orientierungswechsel respektiert. Die Orientierung ist am fünften Polynom, der Determinante, ablesbar. Die drei Längenquadrate und die Determinante bestimmen die orientierte Kongruenzklasse des Dreiecks eindeutig, somit repräsentieren diese vier Funktionen die Quotientenabbildung. Das Quadrat der Determinante kann man als Polynom in den Längenquadraten ausdrücken (beispielsweise ausgehend von der *Heronschen Flächenformel*).

Lemma 5.4. *Die Drehgruppe*

$$\mathrm{SO}_2(\mathbb{R}) \;=\; \left\{ \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} \mid \alpha \in [0, 2\pi) \right\}$$

operiere linear und simultan auf dem $\mathbb{R}^4 = \mathbb{R}^2 \times \mathbb{R}^2$. *Dann ist der Invariantenring der zugehörigen Operation auf dem Polynomring* $\mathbb{R}[U_1, V_1, U_2, V_2]$ *gleich*

$$\mathbb{R}[U_1, V_1, U_2, V_2]^{\mathrm{SO}_2(\mathbb{R})} \;=\; \mathbb{R}[U_1^2 + V_1^2, U_2^2 + V_2^2, U_1U_2 + V_1V_2, U_1V_2 - U_2V_1].$$

Dabei sind die ersten drei Erzeuger algebraisch unabhängig, und das Quadrat von $U_1V_2 - U_2V_1$ *lässt sich durch die ersten drei Erzeuger ausdrücken.*

Beweis. Die Invarianz der angegebenen Polynome sowie ihre inhaltliche Bedeutung wurden schon in Beispiel 5.3 bemerkt. Wir betrachten die Erweiterung

$$\mathbb{R}[U_1, V_1, U_2, V_2] \;\subset\; \mathbb{C}[U_1, V_1, U_2, V_2].$$

Die angegebene Operation der $\mathrm{SO}_2(\mathbb{R})$ auf dem reellen Polynomring lässt sich direkt auf den komplexen Polynomring fortsetzen, da das Gruppenelement

$$\sigma \;=\; \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}$$

durch $U_i \mapsto \cos\alpha\, U_i - \sin\alpha\, V_i$ etc. wirkt, und diese Ringhomomorphismen reell oder komplex aufgefasst werden können.[5] Ein Polynom $F \in \mathbb{R}[U_1, V_1, U_2, V_2]$ ist genau dann invariant, wenn es aufgefasst in $\mathbb{C}[U_1, V_1, U_2, V_2]$ invariant ist. Wir führen neue komplexe Variablen ein, nämlich

$$W_1 = U_1 + iV_1,\; Z_1 = U_1 - iV_1,\; W_2 = U_2 + iV_2,\; Z_2 = U_2 - iV_2\,.$$

Es bestehen die Beziehung

$$\begin{aligned} W_1Z_1 \;&=\; (U_1 + iV_1)\,(U_1 - iV_1) \;=\; U_1^2 + V_1^2, \\ W_2Z_2 \;&=\; (U_2 + iV_2)\,(U_2 - iV_2) \;=\; U_2^2 + V_2^2, \\ W_1Z_2 \;=\; (U_1 + iV_1)\,(U_2 - iV_2) \;&=\; U_1U_2 + V_1V_2 - i\,(U_1V_2 - U_2V_1) \end{aligned}$$

und

$$W_2Z_1 \;=\; (U_2 + iV_2)\,(U_1 - iV_1) \;=\; U_1U_2 + V_1V_2 + i\,(U_1V_2 - U_2V_1)\,.$$

[5] Die operierende Gruppe wird also nicht komplexifiziert.

Die beiden letzten Gleichungen zeigen, dass sich umgekehrt auch $U_1U_2 + V_1V_2$ und $U_1V_2 - U_2V_1$ durch W_1Z_2 und W_2Z_1 ausdrücken lassen. Die beiden Systeme erzeugen also die gleiche $\mathbb{C}$-Unteralgebra von

$$\mathbb{C}[U_1, V_1, U_2, V_2] \cong \mathbb{C}[W_1, Z_1, W_2, Z_2].$$

Wir schreiben die Elemente der operierenden Gruppe als

$$\sigma = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} = \cos\alpha + i\sin\alpha,$$

wobei wir die Drehgruppe mit den komplexen Zahlen vom Betrag 1 (zusammen mit der komplexen Multiplikation) identifizieren. Die Operation wird dann zu ($\bullet$ bezeichne die aus dem Reellen fortgesetzte Operation und $\cdot$ die komplexe Multiplikation)

$$\begin{aligned} W_1 \bullet \sigma &= (U_1 + iV_1) \bullet \sigma \\ &= (\cos\alpha)\, U_1 - (\sin\alpha)\, V_1 + i\,((\sin\alpha)\, U_1 + (\cos\alpha)\, V_1) \\ &= (U_1 + iV_1)\,(\cos\alpha + i\sin\alpha) \\ &= W_1 \cdot \sigma \end{aligned}$$

(ebenso für W_2) und

$$\begin{aligned} Z_1 \bullet \sigma &= (U_1 - iV_1) \bullet \sigma \\ &= (\cos\alpha)\, U_1 - (\sin\alpha)\, V_1 - i\,((\sin\alpha)\, U_1 + (\cos\alpha)\, V_1) \\ &= (U_1 - iV_1)\,(\cos\alpha - i\sin\alpha) \\ &= Z_1 \cdot \sigma^{-1} \end{aligned}$$

(ebenso für Z_2). Wir betrachten auf $\mathbb{C}[W_1, Z_1, W_2, Z_2]$ die $\mathbb{Z}$-Graduierung[6], bei der W_1, W_2 den Grad 1 und Z_1, Z_2 den Grad -1 bekommen. Die Operation der Gruppe ist homogen bezüglich dieser Graduierung. Daher ist der Invariantenring ein graduierter Unterring. Auf der d-ten Stufe des Ringes ist die Operation für $t \in S^1 \subset \mathbb{C}^\times$ durch $H \mapsto t^d H$ gegeben. Für $d = 0$ ist dies die Identität, so dass die 0-te Stufe invariant ist. Für $d \neq 0$ gibt es $t \in S^1$ mit $t^d \neq 1$, so dass es außer 0 keine weiteren invarianten Polynome gibt. Der Invariantenring ist also die 0-te Stufe. Diese besteht aus Linearkombinationen von Monomen der 0-ten Stufe, und ein Monom vom nullten Grad muss ein Produkt der Elemente W_iZ_j sein. Der Invariantenring ist also

$$\begin{aligned} \mathbb{C}[W_1, Z_1, W_2, Z_2]^{\mathrm{SO}_2(\mathbb{R})} &= \mathbb{C}[W_1Z_1, W_1Z_2, W_2Z_1, W_2Z_2] \\ &= \mathbb{C}[U_1^2 + V_1^2, U_2^2 + V_2^2, U_1U_2 + V_1V_2, U_1V_2 - U_2V_1]. \end{aligned}$$

Wir kehren zur reellen Situation zurück. Es sei $F \in \mathbb{R}[U_1, V_1, U_2, V_2]$ ein invariantes Polynom. Dann gibt es ein komplexes Polynom P in vier Variablen mit

$$F = P(U_1^2 + V_1^2, U_2^2 + V_2^2, U_1U_2 + V_1V_2, U_1V_2 - U_2V_1).$$

[6]Wir werden Graduierungen mit einer beliebigen graduierenden Gruppe und die zugehörige Operation der Charaktergruppe in der siebten Vorlesung besprechen.

Mit Hilfe der komplexen Konjugation sieht man, dass es auch ein reelles Polynom mit dieser Eigenschaft geben muss. Daher gilt für den reellen Invariantenring

$$\mathbb{R}[U_1, V_1, U_2, V_2]^{\mathrm{SO}_2(\mathbb{R})} = \mathbb{R}[U_1^2 + V_1^2, U_2^2 + V_2^2, U_1U_2 + V_1V_2, U_1V_2 - U_2V_1].$$

Für den Zusatz siehe Aufgabe 5.4. □

Der folgende Satz ist die polynomial-invariantentheoretische Version der Aussage, dass die Kongruenzklasse eines Dreiecks durch die drei Seitenlängen (SSS) bzw. einen Winkel und zwei anliegende Seitenlängen (SWS) festgelegt ist. Aufgrund dieses elementar-geometrischen Satzes weiß man, dass man jede Invariante der Kongruenzklasse eines Dreiecks „irgendwie“ als eine Funktion der drei Längen ausdrücken kann. Daraus folgt aber keineswegs automatisch, dass man eine polynomiale Invariante auch polynomial ausdrücken kann.

Satz 5.5. *Die orthogonale Gruppe* $\mathrm{O}_2(\mathbb{R})$ *(der Drehungen und der Drehspiegelungen) operiere linear und simultan auf dem*

$$\mathbb{R}^4 = \mathbb{R}^2 \times \mathbb{R}^2.$$

Dann ist der Invariantenring der zugehörigen Operation auf dem Polynomring $\mathbb{R}[U_1, V_1, U_2, V_2]$ *gleich*

$$\mathbb{R}[U_1, V_1, U_2, V_2]^{\mathrm{O}_2(\mathbb{R})} = \mathbb{R}[U_1^2 + V_1^2, U_2^2 + V_2^2, U_1U_2 + V_1V_2].$$

Die drei Erzeuger sind dabei algebraisch unabhängig. Jede polynomiale Invariante eines (nummerierten) Dreieckes lässt sich polynomial in den drei Seitenquadraten ausdrücken.

Beweis. Wie in Beispiel 5.3 erwähnt, gibt es eine kurze exakte Sequenz

$$1 \longrightarrow \mathrm{SO}_2(\mathbb{R}) \longrightarrow \mathrm{O}_2(\mathbb{R}) \longrightarrow \{1, -1\} \longrightarrow 1\,.$$

Wir können daher aufgrund von Proposition 5.1 den Invariantenring

$$\mathbb{R}[U_1, V_1, U_2, V_2]^{\mathrm{O}_2(\mathbb{R})}$$

aus dem Invariantenring zu

$$\mathbb{R}[U_1, V_1, U_2, V_2]^{\mathrm{SO}_2(\mathbb{R})}$$

ausrechnen, der in Lemma 5.4 zu

$$B = \mathbb{R}[U_1^2 + V_1^2, U_2^2 + V_2^2, U_1U_2 + V_1V_2, U_1V_2 - U_2V_1]$$

bestimmt wurde. Das nichttriviale Element der Restklassengruppe $\{1, -1\}$ wirkt auf B durch einen beliebigen Repräsentanten, beispielsweise durch die Spiegelung $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. Der zugehörige Ringautomorphismus lässt U_1, U_2 unverändert und schickt V_1, V_2 auf ihr Negatives. Unter dieser Abbildung sind die drei vorderen Erzeuger invariant und der hintere Erzeuger wird auf sein Negatives abgebildet. Da das Quadrat des vierten Erzeugers zu $A = \mathbb{R}[U_1^2 + V_1^2, U_2^2 + V_2^2, U_1U_2 + V_1V_2]$ gehört, liegt eine Operation auf einem

Ring der Form $A[X]/(X^2-a)$ durch $X \leftrightarrow -X$ vor. In einem solchen Fall ist A der Invariantenring. $\square$

Quotientenkörper von Invariantenringen

Proposition 5.6. *Es sei G eine Gruppe, die auf einem Integritätsbereich R als Gruppe von Ringautomorphismen operiere. Dann gelten folgende Eigenschaften.*

(1) *Der Invariantenring R^G ist ein Integritätsbereich.*
(2) *Die Operation induziert eine Operation von G auf dem Quotientenkörper $Q(R)$ als Gruppe von Körperautomorphismen.*
(3) *Es ist $Q\left(R^G\right) \subseteq (Q(R))^G$.*
(4) *Es ist*
$$R \cap (Q(R))^G = R^G.$$

Beweis. (1) ist wegen $R^G \subseteq R$ klar. (2). Es sei $K = Q(R)$ der Quotientenkörper von R. Zu jedem $\sigma \in G$ setzt sich der Ringautomorphismus $f \mapsto f\sigma$ aufgrund der universellen Eigenschaft der Nenneraufnahme zu einem Körperautomorphismus $\frac{f}{g} \mapsto \frac{f\sigma}{g}$ fort. (3). Ein Element aus dem Quotientenkörper $Q\left(R^G\right)$ hat die Form $\frac{f}{g}$ mit invarianten Elementen $f, g \in R^G$. Es ist also insbesondere invariant unter der induzierten Operation auf K. Daher gilt $Q\left(R^G\right) \subseteq (Q(R))^G$. (4). Die Inklusion $R^G \subseteq R \cap Q(R)^G$ ist direkt klar. Die andere Inklusion ergibt sich, da die Operation von G auf $Q(R)$ eingeschränkt auf R die ursprüngliche Operation ist. Wenn also $f \in R$ ist und aufgefasst in $Q(R)$ invariant ist, so ist es überhaupt invariant. $\square$

Bemerkung 5.7. Mit Proposition 5.6 hängt die Invariantentheorie von Integritätsbereichen eng mit der Galoistheorie des Quotientenkörpers zusammen. In der Situation des Satzes ist bei endlichem G die Körpererweiterung $K^G \subseteq K$ eine Galoiserweiterung, wie aus dem Satz von Artin folgt. K^G ist ja gerade der Fixring unter den Körperautomorphismen zu G. Die Untergruppen $H \subseteq G$ liefern Zwischenkörper $K^G \subseteq M = K^H \subseteq K$ und $M \cap R = R^H$ ist der zugehörige Zwischenring (man darf aber nicht erwarten, dass es eine bijektive Korrespondenz zwischen Zwischenringen und Untergruppen gibt). Häufig besitzen Aussagen der Invariantentheorie stärkere Analoga aus der Galoistheorie. Zu Proposition 5.1 (3) vergleiche man etwa die Rückrichtung von Satz 16.4 (Körper- und Galoistheorie (Osnabrück 2011)) (1).

Es gibt aber auch erhebliche Unterschiede zwischen Invariantentheorie und Galoistheorie. Beispielsweise geht man in der klassischen Galoistheorie eher von einem Grundkörper K aus und untersucht Körpererweiterungen $K \subseteq L$ zusammen mit der K-Automorphismengruppe, während man in der klassischen Invariantentheorie eher mit dem Erweiterungsring anfängt und versucht, die Fixringe zu einer gewissen Operation zu bestimmen. Auch in der

Invariantentheorie wird häufig ein Grundkörper k vorausgesetzt, doch tritt dieser kaum als Invariantenring auf, sondern übernimmt die Rolle, dass alle beteiligten Ringe k-Algebren über diesem Körper und alle Ringhomomorphismen k-Algebrahomomorphismen sind. Beispielsweise ist die Bestimmung von Invariantenringen zum Polynomring $k[X_1, \ldots, X_n]$ zu (linearen) Gruppenoperationen schon ein riesiges Teilgebiet der Invariantentheorie.

Bei einer endlichen Gruppe gilt in Proposition 5.6 (3) sogar Gleichheit, wie die folgende Aussage zeigt.

Lemma 5.8. *Es sei G eine endliche Gruppe, die auf einem Integritätsbereich als Gruppe von Ringautomorphismen operiere. Dann ist*

$$Q\left(R^G\right) = (Q(R))^G.$$

Beweis. Die Inklusion $Q\left(R^G\right) \subseteq (Q(R))^G$ gilt nach Proposition 5.6 (3) für jede Gruppe. Zum Beweis der Umkehrung seien $f, g \in R$, $g \neq 0$, mit $\frac{f}{g} \in (Q(R))^G$ gegeben. Wir betrachten

$$h = \prod_{\sigma \in G,\, \sigma \neq e_G} g\sigma.$$

Dann gelten in $Q(R)$ die Identitäten

$$\begin{aligned} \frac{f}{g} &= \frac{hf}{hg} \\ &= \frac{hf}{\left(\prod_{\sigma \in G,\, \sigma \neq e_G} g\sigma\right) g} \\ &= \frac{hf}{\prod_{\sigma \in G} g\sigma}. \end{aligned}$$

Nach Voraussetzung ist der Bruch und in dieser Darstellung offenbar auch der Nenner invariant. Also muss auch der Zähler invariant sein und somit ist $\frac{f}{g} \in Q\left(R^G\right)$. □

Beispiel 5.9. Es sei K ein unendlicher Körper. Wir betrachten auf $R = K[X, Y]$ die Operation von $K^\times$ durch skalare Multiplikation. Zu $\lambda \in K^\times$ gehört also der durch $X \mapsto \lambda X$, $Y \mapsto \lambda Y$ gegebene K-Algebrahomomorphismus. Der Invariantenring dazu ist K, also ein Körper. Der Quotientenkörper von $K[X, Y]$ ist der Funktionenkörper $K(X, Y)$ in zwei Variablen. Sein Invariantenring unter der Operation ist $K\left(\frac{X}{Y}\right)$, also der Funktionenkörper in einer Variablen. In dieser Situation gilt also

$$Q\left(R^G\right) \neq (Q(R))^G.$$

5. Arbeitsblatt

Aufwärmaufgaben

Aufgabe 5.1. Es sei V ein endlichdimensionaler reeller Vektorraum und $w \in V$ ein fixierter Vektor.

a) Zeige, dass durch

$$\mathbb{R} \times V \longrightarrow V,\, (t,v) \longmapsto v + tw,$$

eine Operation von $(\mathbb{R}, +)$ auf V definiert ist.

b) Zeige, dass eine differenzierbare Funktion

$$f\colon\, V \longrightarrow \mathbb{R}$$

genau dann unter dieser Operation invariant ist, wenn für die Richtungsableitung in Richtung w die Beziehung $D_w f = 0$ gilt.

Aufgabe 5.2. Es sei G eine Gruppe, die auf einer Menge M operiere, und es sei $H \subseteq G$ ein Normalteiler. Zeige, dass auf dem Bahnenraum $M\backslash H$ die Restklassengruppe G/H in natürlicher Weise operiert, und dass der Bahnenraum $(M\backslash H) \setminus (G/H)$ mit dem Bahnenraum $M\backslash G$ übereinstimmt.

Aufgabe 5.3. Es sei K ein Körper, G eine Gruppe und

$$\rho\colon\, G \longrightarrow \mathrm{GL}_V$$

eine Darstellung von G in einen n-dimensionalen Vektorraum über K. Es seien $u_1, \ldots, u_n$ und $v_1, \ldots, v_n$ zwei Basen von V und

$$\rho_u, \rho_v\colon\, G \longrightarrow \mathrm{GL}_n(K)$$

seien die zugehörigen Matrixdarstellungen. Zeige, dass die Invariantenringe $K[X_1, \ldots, X_n]^{G,\rho_u}$ und $K[Y_1, \ldots, Y_n]^{G,\rho_v}$ isomorph sind.

Aufgabe 5.4. Beweise den Zusatz von Lemma 5.4.

Aufgabe 5.5. Zeige, dass der im Beweis zu Lemma 5.4 verwendete komplexe Invariantenring nicht faktoriell ist.

Aufgabe 5.6. Erstelle eine Version von Lemma 5.8 für geeignete multiplikative Systeme.

Aufgabe 5.7. Diskutiere Beispiel 5.9 für den Fall, dass K ein endlicher Körper ist.

Aufgabe 5.8. Man gebe ein Beispiel für einen Integritätsbereich R und einer Gruppenoperation einer endlichen Gruppe G auf R derart, dass nicht jeder Zwischenring S, $R^G \subseteq S \subseteq R$, der Invariantenring zu einer Untergruppe von G ist.

Aufgaben zum Abgeben

Aufgabe 5.9. (4 Punkte)

Wir betrachten die natürliche Operation der Drehgruppe SO_2 auf dem $\mathbb{R}^4 = (\mathbb{R}^2)^2$. Mit den natürlichen Identifizierungen $\mathbb{C} \cong \mathbb{R}^2$ und

$$\mathrm{SO}_2 \cong \{u \in \mathbb{C} | \ |u| = 1\}$$

kann man dies als eine lineare Operation auf dem $\mathbb{C}^2$ auffassen. Zeige, dass die zugehörige Operation auf dem Polynomring $\mathbb{C}[w, z]$ nur die Konstanten als Invarianten besitzt.

Aufgabe 5.10. (5 Punkte)

Drücke die Funktion

$$\mathbb{R}^2 \longrightarrow \mathbb{R}, (x, y) \longmapsto x^2,$$

explizit als eine stetige Funktion in den Funktionen xy und $x^2 - y^2$ aus.

(vergleiche Aufgabe 4.14).

Aufgabe 5.11. (6 Punkte)

Es sei K ein unendlicher Körper. Wir betrachten auf dem Körper $K(X, Y)$ die Operation von $K^\times$, wobei $\lambda \in K^\times$ durch $X \mapsto \lambda X$, $Y \mapsto \lambda Y$ auf $K[X, Y]$ wirkt und diese Wirkung auf den Quotientenkörper fortgesetzt wird. Zeige, dass der Fixring zu dieser Operation gleich $K\left(\frac{X}{Y}\right)$ ist.

Aufgabe 5.12. (3 Punkte)

Es sei $\mathbb{K} = \mathbb{R}$ oder $\mathbb{C}$. Wir betrachten die skalare Multiplikation von $\mathbb{K}^\times$ auf $\mathbb{K}^n$. Es sei Y ein metrischer Raum und

$$\varphi\colon \mathbb{K}^n \longrightarrow Y$$

eine stetige Abbildung, die auf den Bahnen der Operation konstant sei. Zeige, dass φ konstant ist.

6. Vorlesung - Der Reynolds-Operator

Die alternierende Gruppe

Wir haben gesehen, dass der Invariantenring zur Operation der symmetrischen Gruppe S_n auf dem Polynomring isomorph zum Polynomring in den elementarsymmetrischen Polynomen ist. Eine wichtige Untergruppe der symmetrischen Gruppe ist die alternierende Gruppe $A_n \subseteq S_n$, an deren Definition wir erinnern.

Definition 6.1. Zu $n \in \mathbb{N}$ heißt die Untergruppe

$$A_n := \{\sigma \in S_n | \operatorname{sgn}(\sigma) = 1\}$$

der geraden Permutationen die *alternierende Gruppe*.

Die alternierende Gruppe ist der Kern des Signumshomomorphismus und damit ein Normalteiler. Die A_n operiert wie die S_n auf dem Polynomring $K[X_1, \ldots, X_n]$. Wir interessieren uns für den Invariantenring $K[X_1, \ldots, X_n]^{A_n}$. Nach Proposition 5.1 (1) haben wir die Inklusionen

$$K[E_1, \ldots, E_n] \cong K[X_1, \ldots, X_n]^{S_n} \subseteq K[X_1, \ldots, X_n]^{A_n} \subseteq K[X_1, \ldots, X_n].$$

Zur Beschreibung des Invariantenringes unter der alternierenden Gruppe ist der Begriff der relativen Invarianten bezüglich eines Charakters sinnvoll.

Relative Invarianten

Definition 6.2. Es sei K ein Körper und R eine kommutative K-Algebra, auf der eine Gruppe G als Gruppe von K-Algebraautomorphismen operiere. Es sei

$$\chi \colon G \longrightarrow K^\times$$

ein Charakter auf G. Dann nennt man

$$R_\chi^G := \{f \in R | f\sigma = \chi(\sigma) \cdot f \text{ für alle } \sigma \in G\}$$

die χ-*relativen Invarianten* oder *Semiinvarianten* bezüglich χ.

Der Invariantenring ist also die Menge der Invarianten relativ zum trivialen Charakter. Die χ-relativen Invarianten sind ein R^G-Untermodul von R. Wenn nämlich g invariant und f χ-invariant ist, so ist

$$(gf)\sigma = (g)\sigma \cdot (f)\sigma = g\chi(\sigma)f.$$

Der Invariantenring zur alternierenden Gruppe

Lemma 6.3. *Es sei K ein Körper der Charakteristik $\neq 2$. Dann gilt für die natürliche Operation der Permutationsgruppe S_n auf dem K^n die Gleichheit*

$$K[X_1, \ldots, X_n]^{S_n}_{\mathrm{sgn}} \;=\; K[X_1, \ldots, X_n]^{S_n} \cdot \triangle,$$

wobei $\triangle = \prod_{j<i}(X_i - X_j)$ die Vandermondesche Determinante ist.

Beweis. Das Polynom $\triangle$ hat offenbar die Eigenschaft, dass es signumsinvariant ist, dass sich also sein Vorzeichen bei einer ungeraden Permutation umkehrt. Hierzu muss man sich nur klar machen, dass sich bei einer Transposition das Vorzeichen um -1 ändert. Dabei kann man sich sogar auf solche Transpositionen beschränken, die zwei Nachbarn i und $i+1$ miteinander vertauschen. Dann wird aus dem Faktor $X_{i+1} - X_i$ der Faktor $X_i - X_{i+1}$ und alle anderen Faktoren werden allenfalls vertauscht. Insgesamt wird $\triangle$ auf $-\triangle$ abgebildet. Wir müssen also zeigen, dass jedes signumsinvariante Polynom F ein Vielfaches von $\triangle$ ist. Der andere Faktor ist dann automatisch invariant.

Für diese Teilerbeziehung genügt es wegen der Faktorialität von $K[V]$ zu zeigen, dass $X_i - X_j$ ein Teiler von F ist $(i \neq j)$. Wir schreiben F in den neuen Variablen $X_k, k \neq i, j, X_i + X_j, X_i - X_j$ als

$$F \;=\; \sum_{n=0}^{m} G_n\left(X_k, X_i + X_j\right)\left(X_i - X_j\right)^n.$$

Dann ist einerseits

$$F(X_i \mapsto X_j) \;=\; \sum_{n=0}^{m} (-1)^n G_n\left(X_k, X_i + X_j\right)\left(X_i - X_j\right)^n$$

und anderseits (da F signumsinvariant ist)

$$F(X_i \mapsto X_j) \;=\; -F \;=\; -\sum_{n=0}^{m} G_n\left(X_k, X_i + X_j\right)\left(X_i - X_j\right)^n.$$

Daraus folgt wegen $\mathrm{char}(K) \neq 2$, dass für n gerade $G_n = 0$ sein muss. Insbesondere ist $G_0 = 0$. Also ist $F = H\left(X_i - X_j\right)$, wie behauptet. □

Noch einmal explizit: Es geht um die Polynome, die relativ zur Signumsabbildung invariant sind, für die also

$$F\sigma \;=\; \mathrm{sgn}(\sigma) F$$

für alle Permutationen gilt. Für eine gerade Permutation σ muss also

$$F\sigma \;=\; F$$

sein, für eine ungerade Permutation dagegen

$$F\sigma \;=\; -F.$$

Insbesondere sind solche Polynome invariant unter der alternierenden Gruppe.

Satz 6.4. *Es sei K ein Körper der Charakteristik* $\mathrm{char}(K) \neq 2$. *Die alternierende Gruppe A_n operiere natürlich auf $V = K^n$. Dann ist*

$$K[V]^{A_n} = K[V]^{S_n} \oplus K[V]^{S_n}_{\mathrm{sgn}} = K[E_1, \ldots, E_n] \oplus K[E_1, \ldots, E_n] \cdot \triangle.$$

Beweis. Die Gleichheit rechts ergibt sich aus Satz 1.7 und Lemma 6.3. Auf $K[V]^{A_n}$ operiert die Restklassengruppe $S_n/A_n = \{1, -1\} = \mathbb{Z}/(2)$ wie in Proposition 5.1 beschrieben. Sei τ das nichttriviale Element daraus. Dieses wird repräsentiert durch eine beliebige ungerade Permutation, etwa durch eine Transposition. Sei $F \in K[V]^{A_n}$ ein Polynom, das invariant unter der alternierenden Gruppe ist. Nach Proposition 5.1 (3) ist $F\tau$ unabhängig von dem gewählten Repräsentanten τ. Es ist

$$F = \frac{1}{2}(F + F\tau) + \frac{1}{2}(F - F\tau),$$

wobei die beiden Summanden symmetrisch bzw. signumsinvariant sind. Dies überprüft man, indem man die (geraden oder ungeraden) Permutationen darauf anwendet. Die Summe ist direkt, da der Durchschnitt 0 ist: Ein Polynom, das sowohl symmetrisch als auch signumsinvariant ist, muss 0 sein. □

Beispiel 6.5. Die natürliche Operation der alternierenden Gruppe $A_3 \cong \mathbb{Z}/(3)$ auf dem K^3 wird durch den Zykel

$$e_1 \longmapsto e_2,\ e_2 \longmapsto e_3,\ e_3 \longmapsto e_1$$

erzeugt. Besitzt K dritte primitive Einheitswurzeln, so kann man die zugehörige Matrix diagonalisieren und man erhält eine neue Basis mit den Eigenvektoren

$$e_1 + e_2 + e_3,\ e_1 + \zeta e_2 + \zeta^2 e_3,\ e_1 + \zeta^2 e_2 + \zeta e_3\,.$$

Wir führen die neuen Variablen

$$U = X + Y + Z,\ V = X + \zeta Y + \zeta^2 Z,\ W = X + \zeta^2 Y + \zeta Z$$

ein. In dieser Basis ist der erzeugende Automorphismus durch

$$U \longmapsto U,\ V \longmapsto \zeta V,\ W \longmapsto \zeta^2 W$$

gegeben und der Invariantenring ist in dieser Basis gleich

$$K[U, V^3, VW, W^3]\,.$$

Die einzige Relation ist gegeben durch $V^3W^3 = (VW)^3$.

Wie sieht der Unterring der symmetrischen Polynome aus? Die Transposition $Y \leftrightarrow Z$ lässt U unverändert und vertauscht V und W. Das bedeutet für den alternierenden Invariantenring, dass V^3 und W^3 vertauscht werden. Der symmetrische Invariantenring ist daher

$$K[U, VW, V^3 + W^3]\,.$$

Dabei sind

$$VW = X^2 + Y^2 + Z^2 + \zeta XY + \zeta^2 XY + \zeta XZ + \zeta^2 XZ + \zeta YZ + \zeta^2 YZ,$$

$$V^3 = X^3 + Y^3 + Z^3 + 6XYZ + 3\xi^2XY^2 + 3\xi X^2Y + 3\xi XZ^2 + 3\xi^2X^2Z + 3\xi^2YZ^2 + 3\xi Y^2Z$$

und

$$W^3 = X^3 + Y^3 + Z^3 + 6XYZ + 3\xi XY^2 + 3\xi^2X^2Y + 3\xi^2XZ^2 + 3\xi X^2Z + 3\xi YZ^2 + 3\xi^2Y^2Z.$$

Für die Vandermondsche Determinante gilt

$$\begin{aligned} \triangle &= (Y-X)(Z-X)(Z-Y) \\ &= XY^2 - X^2Y + X^2Z - XZ^2 + YZ^2 - Y^2Z \\ &= \frac{1}{3(\xi^2-\xi)}\left(V^3 - W^3\right). \end{aligned}$$

Reynolds-Operator

Definition 6.6. Es sei $R \subseteq S$ ein Unterring eines kommutativen Ringes S. Man sagt, das R ein *direkter Summand* von S ist, wenn es einen R-Modul M gibt mit $S \cong R \oplus M$ (es liegt also ein R-Modulisomorphismus vor).

Diese Eigenschaft ist äquivalent dazu, dass es einen R-Modulhomomorphismus

$$\psi\colon\ S \longrightarrow R$$

mit $\psi \circ \iota = \mathrm{id}_R$ gibt. Eine stärkere Eigenschaft ist die Existenz eines Ringhomomorphismus

$$\psi\colon\ S \longrightarrow R$$

mit $\psi \circ \iota = \mathrm{id}_R$.

Beispiel 6.7. Es sei K ein Körper und A eine von 0 verschiedene K-Algebra. Dann ist K ein direkter Summand von A. Dies beruht darauf, dass man die 1 zu einer K-Basis von A ergänzen kann. Mit dem von den anderen Basiselementen erzeugten K-Untervektorraum $V \subset A$ ist dann $A \cong K \cdot 1 \oplus V$. Im Allgemeinen muss es aber keinen K-Algebrahomomorphismus $A \to K$ geben. Bei einer (nichttrivialen) Körpererweiterung $K \subset L$ gibt es keinen Ringhomomorphismus von L nach K.

Für einen Invariantenring $R^G \subseteq R$ nennt man einen R^G-Modulhomomorphismus

$$\rho\colon\ R \longrightarrow R^G$$

mit $\rho \circ \iota = \mathrm{Id}_{R^G}$ auch einen *Reynolds-Operator*. Ein Reynolds-Operator muss im Allgemeinen nicht existieren, er existiert aber unter der folgenden Bedingung.

Lemma 6.8. *Es sei G eine endliche Gruppe, die auf einer kommutativen K-Algebra R als Gruppe von K-Algebraautomorphismen operiere. Die Gruppenordnung sei kein Vielfaches der Charakteristik von K. Dann ist die Abbildung*

$$\rho\colon\ R \longrightarrow R^G,\ f \longmapsto \frac{1}{\#(G)} \sum_{\sigma \in G} f\sigma,$$

ein Reynolds-Operator. Insbesondere ist $R^G \subseteq R$ ein direkter Summand.

Beweis. Aufgrund der Voraussetzung an die Charakteristik ist $\#(G)$ eine Einheit in K und damit in R, also ist die angegebene Abbildung wohldefiniert. Die Abbildung ist offenbar ein Gruppenhomomorphismus. Für $g \in R^G$ und $f \in R$ ist ferner

$$\begin{aligned}
\rho(gf) &= \frac{1}{\#(G)} \sum_{\sigma \in G} (gf)\sigma \\
&= \frac{1}{\#(G)} \sum_{\sigma \in G} (g\sigma)(f\sigma) \\
&= \frac{1}{\#(G)} \sum_{\sigma \in G} g(f\sigma) \\
&= g\left(\frac{1}{\#(G)} \sum_{\sigma \in G} f\sigma \right) \\
&= g\rho(f),
\end{aligned}$$

daher liegt ein R^G-Modulhomomorphismus vor. Für $g \in \mathbb{R}^G$ ist

$$\rho(g) \ = \ \frac{1}{\#(G)} \sum_{\sigma \in G} g\sigma \ = \ \frac{1}{\#(G)} \sum_{\sigma \in G} g \ = \ \frac{1}{\#(G)} \left(\#(G)g\right) \ = \ g,$$

also ist

$$\rho \circ \iota \ = \ \mathrm{Id}_{R^G}\,.$$

□

Die Bedingung, dass die Gruppenordnung zur Charakteristik teilerfremd ist, ist für viele Resultate der Invariantentheorie eine wesentliche Voraussetzung. Der andere Fall, dass die Gruppenordnung ein Vielfaches der Charakteristik ist, bildet ein eigenes Kapitel der Invariantentheorie, und besitzt sogar einen eigenen Namen. Man spricht von *modularer Invariantentheorie*.

Beispiel 6.9. Es sei K ein Körper der Charakteristik 0 und $A = K[X, Y]$. Auf der A-Algebra

$$B \ = \ A[S,T]/(XS + YT + 1) \ = \ K[X, Y, S, T]/(XS + YT + 1)$$

operiert die additive Gruppe $(K, +)$, indem ein $\lambda \in K$ durch

$$X \mapsto X,\ Y \mapsto Y,\ S \mapsto S + \lambda Y,\ T \mapsto T - \lambda X$$

wirkt. Wegen

$$X(S+\lambda Y)+Y(T-\lambda X) \;=\; XS+YT \;=\; -1$$

sind diese zunächst auf $K[X,Y,S,T]$ definierten Ringautomorphismen auch auf der Restklassenalgebra Automorphismen. Der Invariantenring ist $A = K[X,Y]$, wobei die Inklusion

$$A \;\subseteq\; B^G$$

unmittelbar klar ist. Zum Beweis der Umkehrung betrachten wir die Nenneraufnahme $A \to A_X$ und $B \to B_X$. Es ist

$$\begin{array}{rcl} B_X & = & (K[X,Y,S,T]/(XS+YT+1))_X \\ & \cong & (A_X[S,T])\,/(XS+YT+1) \\ & \cong & A_X[T], \end{array}$$

wobei beim letzten Isomorphismus S auf $\frac{-1-YT}{X}$ abgebildet wird. Ebenso ist $B_Y \cong A_Y[S]$. Die Operation lässt sich auf diese beiden Nenneraufnahmen fortsetzen. Für die Operation auf $B_X = A_X[T]$ ist A_X der Invariantenring. Zu einem $\lambda \in K$, $\lambda \neq 0$, wird ein Polynom

$$F \;=\; a_0 + a_1T + \ldots + a_{n-1}T^{n-1} + a_nT^n$$

auf

$$a_0 + a_1(T-\lambda X) + \ldots + a_{n-1}(T-\lambda X)^{n-1} + a_n(T-\lambda X)^n$$

abgebildet. Bei $n \geq 1$ ist der Koeffizient zu T^{n-1}

$$a_{n-1} - n\lambda X a_n$$

und dies ist bei $\lambda \neq 0$ nicht gleich a_{n-1}. Also ist ein solches Polynom nicht invariant. Das gleiche Argument gilt für $A_Y \subseteq A_Y[S] = B_Y$.

Es sei nun $F \in B$ invariant. Dann ist F auch als Element in B_X bzw. in B_Y invariant und daher ist sowohl $F \in A_Y$ als auch $F \in A_X$. Aus

$$F \;=\; \frac{G}{X^n} \;=\; \frac{H}{Y^m}$$

folgt

$$GY^m \;=\; HX^n$$

und aus der Faktorialität von $K[X,Y]$ ergibt sich, dass G ein Vielfaches von X^n sein muss. Somit gehört F zu A. Der Invariantenring ist also A. Dieser ist aber kein direkter Summand in B. Es ist $1 \notin (X,Y)$ in A, aber $1 \in (X,Y)$ in B, was unmittelbar aus der definierenden Gleichung $XS+YT=-1$ folgt. Nach Aufgabe 6.10 kann daher kein direkter Summand vorliegen.

6. Arbeitsblatt

Aufwärmaufgaben

Aufgabe 6.1. Sei $M = \{1, \ldots, n\}$ und sei σ eine Permutation auf M. Die zugehörige *Permutationsmatrix* M_σ ist dadurch gegeben, dass

$$a_{\sigma(i),i} = 1$$

ist und alle anderen Einträge null sind. Zeige, dass

$$\det(M_\sigma) = \operatorname{sgn}(\sigma)$$

ist.

Aufgabe 6.2. Man mache sich klar, dass die symmetrische Gruppe S_3 die uneigentliche Symmetriegruppe eines gleichseitigen Dreiecks ist und die alternierende Gruppe A_3 dabei die eigentliche Symmetriegruppe ist. Ebenso für die S_4, die A_4 und das (gleichseitige) Tetraeder.

Aufgabe 6.3. Wie findet man die in Aufgabe 6.2 angesprochenen Figuren in der natürlichen Operation der S_3 bzw. S_4 auf dem $\mathbb{R}^3$ bzw. $\mathbb{R}^4$ wieder?

Man denke an Aufgabe 3.16.

Aufgabe 6.4. Drücke das Quadrat der Vandermondschen Determinante mit den elementarsymmetrischen Polynomen aus.

Aufgabe 6.5. Es sei K ein Körper und R eine kommutative K-Algebra, auf der eine Gruppe G als Gruppe von K-Algebraautomorphismen operiere. Zeige, dass ein Element $f \in R$, $f \neq 0$, allenfalls bezüglich eines Charakters semiinvariant sein kann.

Es sei M eine Menge, auf der eine Gruppe G operiere. Eine Teilmenge $T \subseteq M$ heißt *G-invariant*, wenn zu jedem $x \in T$ und jedem $\sigma \in G$ auch $\sigma x \in T$ gilt.

Aufgabe 6.6. Es sei M eine Menge, auf der eine Gruppe G operiere und es sei $T \subseteq M$ eine Teilmenge. Zeige, dass T genau dann eine G-invariante Teilmenge ist, wenn T eine Vereinigung von Bahnen ist.

Aufgabe 6.7. Es sei M eine Menge, auf der eine Gruppe G operiere. Es sei $T \subseteq M$ eine G-invariante Teilmenge. Zeige die folgenden Aussagen.

(1) Es gibt eine natürliche Abbildung
$$\varphi\colon\ T\backslash G \longrightarrow M\backslash G$$
zwischen den Bahnenräumen.
(2) Die Abbildung φ ist injektiv.
(3) Die Abbildung φ muss nicht surjektiv sein.

Aufgabe 6.8. Es sei R ein kommutativer Ring, auf dem eine Gruppe G als Gruppe von Ringautomorphismen operiere. Es sei $\mathfrak{a} \subseteq R$ ein Ideal, das unter der Gruppenoperation invariant ist (es gelte also $f\sigma \in \mathfrak{a}$ für $f \in \mathfrak{a}$ und jedes $\sigma \in G$). Zeige die folgenden Aussagen.

(1) Es gibt eine natürliche Operation von G auf dem Restklassenring $R/\mathfrak{a}$.
(2) Es gibt einen Ringhomomorphismus
$$\psi\colon\ R^G/\left(\mathfrak{a} \cap R^G\right) \longrightarrow (R/\mathfrak{a})^G\,.$$
(3) Die Abbildung ψ aus Teil (2) ist injektiv.
(4) Wenn G endlich ist und R einen Körper der Charakteristik 0 enthält, so ist ψ surjektiv.

Aufgabe 6.9. Zeige durch ein Beispiel, dass der Reynolds-Operator zur Operation einer endlichen Gruppe auf einem kommutativen Ring kein Ringhomomorphismus sein muss.

Aufgabe 6.10. Es sei $R \subseteq S$ ein direkter Summand von kommutativen Ringen. Es sei $I \subseteq R$ ein Ideal und $f \in R$. Zeige, dass aus $f \in IS$ die Zugehörigkeit $f \in I$ folgt.

Aufgabe 6.11. Es seien R und S kommutative Ringe, wobei R ein direkter Summand von S sei, sagen wir $S = R \oplus V$ mit einem R-Modul V. Zeige, dass für ein multiplikatives System $M \subseteq R$ die Beziehung
$$S_M \ = \ R_M \oplus V_M$$
gilt.

Aufgabe 6.12. Es seien R und S kommutative Ringe, wobei R ein direkter Summand von S sei, sagen wir $S = R \oplus V$ mit einem R-Modul V. Zeige, dass für ein Ideal $I \subseteq R$ die Beziehung
$$S/IS \ = \ R/I \oplus V/IV$$
gilt.

Aufgabe 6.13. Betrachte die Operation der symmetrischen Gruppe S_n auf dem Polynomring $R = K[X_1, \ldots, X_n]$ über einem Körper K. Bestimme (zu $n = 2, 3, 4$ und in geeigneter Charakteristik) für jede Untergruppe $H \subseteq S_n$ den Reynolds-Operator von R nach R^H.

In Beispiel 6.9 trat eine sogenannte *erzwingende Algebra* auf.

Aufgabe 6.14. Sei R ein kommutativer Ring und sei $\mathfrak{a} = (f_1, \ldots, f_n)$ ein endlich erzeugtes Ideal. Es sei $f \in R$ ein weiteres Element. Dann nennt man die R-Algebra

$$A = R[T_1, \ldots, T_n]/(f_1T_1 + \ldots + f_nT_n + f)$$

die *erzwingende Algebra* zu den $f_1, \ldots, f_n, f$. Zeige, dass A folgende Eigenschaft erfüllt: Zu jedem Ringhomomorphismus $\varphi : R \to S$ in einen kommutativen Ring S mit der Eigenschaft $\varphi(f) \in \mathfrak{a}S$ gibt es einen R-Algebrahomomorphismus $\vartheta : A \longrightarrow S$. Zeige ebenso, dass dieser Homomorphismus *nicht* eindeutig bestimmt ist.

Aufgaben zum Abgeben

Aufgabe 6.15. (3 Punkte)

Es sei K ein unendlicher Körper und $R = K[X_1, \ldots, X_n]$ der Polynomring über K mit der Standardgraduierung. Die Einheitengruppe $K^\times$ operiert linear auf K^n und auf dem Polynomring durch skalare Multiplikation. Zeige, dass die d-te Stufe R_d mit dem Raum der relativen Invarianten bezüglich des Charakters

$$K^\times \longrightarrow K^\times,\ z \longmapsto z^d,$$

übereinstimmt.

Aufgabe 6.16. (5 Punkte)

Es sei R ein kommutativer Ring, auf dem eine endliche Gruppe G als Gruppe von Ringautomorphismen operiere. Zeige die folgenden Aussagen.

(1) Zu jedem $k \in \mathbb{N}$ und jedem $f \in R$ ist der Ausdruck

$$\psi_k(f) = \sum_{T \subseteq G,\, \#(T)=k} \prod_{\sigma \in T} f\sigma$$

invariant.

(2) Wenn R einen Körper der Charakteristik 0 enthält, so erzeugen die $\psi_k(f)$, $f \in R$, $k \in \mathbb{N}$, den Invariantenring.

(3) Teil (2) gilt nicht ohne die Voraussetzung an die Charakteristik.

Aufgabe 6.17. (5 Punkte)

Es sei G eine endliche Gruppe, die auf einem kommutativen Ring R als Gruppe von Ringautomorphismen operiere, wobei die Ordnung von G eine Einheit in R sei. Es sei $H \subseteq G$ ein Normalteiler. Es sei ρ der Reynolds-Operator zu G, δ der Reynolds-Operator zu H und γ der Reynolds-Operator zur Operation von G/H auf R^H (siehe Proposition 5.1). Zeige

$$\rho = \gamma \circ \delta.$$

7. Vorlesung - Graduierungen

Wir haben schon vereinzelt die Standardgraduierung auf dem Polynomring verwendet. In dieser Vorlesung führen wir graduierte Ringe allgemein ein und erläutern den engen Zusammenhang zwischen Graduierungen und Gruppenoperationen vom kommutativen Gruppen.

Graduierungen

Definition 7.1. Es sei R ein kommutativer Ring und D eine kommutative Gruppe. Eine R-Algebra A heißt *D-graduiert*, wenn es eine direkte Summenzerlegung

$$A = \bigoplus_{d \in D} A_d$$

mit R-Untermoduln A_d gibt derart, dass $R \subseteq A_0$ ist und für die Multiplikation auf A die Beziehung

$$A_d \cdot A_e \subseteq A_{d+e}$$

gilt.

Eine einfache Überlegung zeigt, dass $1 \in A_0$ ist und dass somit A_0 eine R-Unteralgebra von A ist. Häufig spricht man einfach von einem D-graduierten Ring A. Statt R kann man stets $\mathbb{Z}$ oder A_0 als Grundring wählen.

Bemerkung 7.2. In einer D-graduierten R-Algebra besitzt jedes Element $a \in A$ eine eindeutige Darstellung

$$a = \sum_{d \in D} a_d \text{ mit } a_d \in A_d\,,$$

wobei nur endlich viele der a_d ungleich 0 sein können. Die a_d heißen dabei die *homogenen Komponenten* von a, die A_d heißen ebenfalls die *homogenen Komponenten* von A (oder d-ten Stufen) und Elemente $a \in A_d$ heißen *homogen* vom *Grad* d. Die Gruppe D heißt die *graduierende Gruppe*. Der Fall $A_d = 0$ ist erlaubt.

Durch eine Graduierung wird die Multiplikation auf einer Algebra A übersichtlicher strukturiert. Man muss lediglich für homogene Elemente $a \in A_d$ und $b \in A_e$ die Produkte $ab \in A_{d+e}$ kennen, dadurch ist schon die gesamte Multiplikation distributiv festgelegt.

Beispiel 7.3. Es sei R ein kommutativer Ring und $R[X_1, \ldots, X_n]$ der Polynomring in n Variablen über R. Dieser ist in naheliegender Weise $\mathbb{Z}$-graduiert. Man definiert für ein Monom $X_1^{k_1} X_2^{k_2} \cdots X_n^{k_n}$ den Grad durch $k_1+k_2+\ldots+k_n$ und setzt A_d als den R-Modul aller Polynome an, die R-Linearkombinationen von Monomen von Grad d sind. Bei der Multiplikation von zwei Monomen verhält sich der Grad offensichtlich additiv, so dass dadurch eine graduierte R-Algebra entsteht. Es ist $A_0 = R$ und $A_n = 0$ für negativen Grad n. Diese Graduierung heißt auch die *Standardgraduierung* auf dem Polynomring.

Beispiel 7.4. Es sei R ein kommutativer Ring und $R[X_1, \ldots, X_n]$ der Polynomring in n Variablen über R. Die additive Gruppe des Polynomrings ist einfach

$$\bigoplus_{\nu \in \mathbb{N}^n} R \cdot X^\nu \, .$$

Daher ist der Polynomring $\mathbb{Z}^n$-graduiert, wobei die $\nu = (\nu_1, \ldots, \nu_n)$-te Stufe einfach aus allen R-Vielfachen des Monoms

$$X^\nu \; = \; X_1^{\nu_1} \cdots X_n^{\nu_n}$$

besteht. Die Stufen zu $\nu \in \mathbb{N}^n$ sind also isomorph zu R, die anderen Stufen, bei denen mindestens eine Komponente negativ ist, sind 0. Diese Graduierung nennt man die *feine Graduierung* des Polynomringes.

Durch einen (surjektiven) Gruppenhomomorphismus

$$\mathbb{Z}^n \longrightarrow D$$

kann man aus der feinen Graduierung des Polynomrings wiederum „gröbere Graduierungen“ gewinnen. In Beispiel 7.13 wird diese Konstruktion eingesetzt.

Beispiel 7.5. Es sei K ein Körper, $a \in K$ und $n \in \mathbb{N}$. Dann besitzt die Restklassenalgebra $A = K[X]/(X^n - a)$ eine Graduierung mit der graduierenden Gruppe $D = \mathbb{Z}/(n)$, und zwar setzt man (wobei x die Restklasse von X sei)

$$A_d = \left\{ \lambda x^d | \, \lambda \in K \right\} \, .$$

Jedes Element $f \in A$ kann man durch ein Polynom repräsentieren, das maximal den Grad $n-1$ besitzt. Daher besitzt jedes f eine Summendarstellung mit Summanden aus den A_d. Diese Summenzerlegung ist direkt, da man mit der einzigen gegebenen Gleichung $X^n = a$ nicht weiter reduzieren kann. Die Multiplikationseigenschaft folgt aus $\lambda x^d \cdot \mu x^e \; = \; \lambda\mu x^{d+e}$, und dies ist gleich $\lambda\mu a x^{d+e-n}$, falls $d + e \geq n$ ist, und andernfalls gleich $\lambda\mu x^{d+e}$. So oder so ist es ein Element aus A_{d+e}.

Lemma 7.6. *Es sei D eine kommutative Gruppe und A ein kommutativer D-graduierter Ring. Dann ist $A_0 \subseteq A$ ein direkter Summand.*

Beweis. Die Stufen A_d sind A_0-Moduln, daher ist

$$A = A_0 \oplus \left(\bigoplus_{d \in D,\, d \neq 0} A_d \right)$$

eine direkte Summenzerlegung. □

Wir nennen die Stufe A_0 auch die *neutrale Stufe* des graduierten Ringes.

Homogene Ideale

Definition 7.7. Es sei R ein kommutativer Ring, D eine kommutative Gruppe und

$$A = \bigoplus_{d \in D} A_d$$

eine D-graduierte R-Algebra. Ein Ideal $\mathfrak{a} \subseteq A$ heißt *homogen*, wenn zu $f \in \mathfrak{a}$ auch die homogenen Komponenten $f_d \in \mathfrak{a}$ sind.

Für ein homogenes Ideal liegt die Summenzerlegung

$$\mathfrak{a} = \bigoplus_{d \in D} \mathfrak{a}_d$$

mit

$$\mathfrak{a}_d = \mathfrak{a} \cap A_d$$

vor.

Lemma 7.8. *Es sei R ein kommutativer Ring, D eine kommutative Gruppe und A eine D-graduierte R-Algebra. Es sei $\mathfrak{a} \subseteq A$ ein homogenes Ideal. Dann ist auch der Restklassenring $R/\mathfrak{a}$ D-graduiert. Dabei ist*

$$(R/\mathfrak{a})_d = R_d/\mathfrak{a}_d.$$

Beweis. Siehe Aufgabe 7.7. □

Graduierungen und Gruppenoperationen

Wir kommen nun zu der Beziehung zwischen D-Graduierungen und Operationen der Charaktergruppe $D^\vee$.

Lemma 7.9. *Es sei K ein Körper, D eine kommutative Gruppe und A eine D-graduierte kommutative K-Algebra. Dann gibt es einen Gruppenhomomorphismus*

$$D^\vee = \mathrm{Char}\,(D, K) \longrightarrow \mathrm{Aut}_K\,(A)\,,\ \chi \longmapsto (a_d \mapsto \chi(d) a_d),$$

der Charaktergruppe von D in die (homogene) K-Automorphismengruppe von A. Wenn alle $A_d \neq 0$ sind, so ist diese Zuordnung injektiv.

Beweis. Zu jedem Charakter

$$\chi\colon\ D \longrightarrow K^\times$$

ist die durch $\varphi_\chi\left(\sum_{d\in D} a_d\right) = \sum_{d\in D} \chi(d)\cdot a_d$ definierte Abbildung φ_χ mit der Addition verträglich. Die Verträglichkeit mit der Multiplikation folgt für homogene Elemente $a_d \in A_d$ und $a_e \in A_e$ aus

$$\varphi_\chi(a_d \cdot a_e) \;=\; \chi(d+e)a_d \cdot a_e \;=\; \chi(d)\cdot\chi(e)a_d\cdot a_e \;=\; \varphi_\chi(a_d)\cdot\varphi_\chi(a_e),$$

woraus sich aufgrund des Distributivgesetzes auch der allgemeine Fall ergibt. Für $a \in A_0$ (und insbesondere für $a \in K$) ist ferner $\varphi_\chi(a) = \chi(0)a = a$, so dass ein K-Algebrahomomorphismus vorliegt. Der triviale (konstante) Charakter geht bei dieser Zuordnung auf die Identität. Es seien nun zwei Charaktere $\chi_1, \chi_2 \in \operatorname{Char}(D, K)$ gegeben. Für ein homogenes Element $a_d \in A_d$ ist

$$\begin{aligned}
\varphi_{\chi_1\cdot\chi_2}(a_d) &= (\chi_1\cdot\chi_2)(d)\cdot a_d \\
&= \chi_1(d)\cdot\chi_2(d)\cdot a_d \\
&= \chi_1(d)\cdot\varphi_{\chi_2}(a_d) \\
&= \varphi_{\chi_1}(\varphi_{\chi_2}(a_d)) \\
&= (\varphi_{\chi_1}\circ\varphi_{\chi_2})(a_d),
\end{aligned}$$

so dass die Gesamtzuordnung mit den Verknüpfungen verträglich ist. Daher gilt auch

$$\varphi_\chi \circ \varphi_{\chi^{-1}} \;=\; \varphi_{\chi\circ\chi^{-1}} \;=\; \varphi_1 \;=\; \mathrm{id}_A,$$

so dass jedes φ_χ ein K-Algebraautomorphismus und die Gesamtzuordnung ein Gruppenhomomorphismus ist. Die Injektivität ergibt sich unter Verwendung von Lemma 4.9 (Körper- und Galoistheorie (Osnabrück 2011)) folgendermaßen. Bei $\chi \neq 1$ gibt es ein $d \in D$ mit $\chi(d) \neq 1$. Nach Voraussetzung ist $A_d \neq 0$, sei also $a \in A_d$, $a \neq 0$. Damit ist $\varphi_\chi(a) = \chi(d)a \neq a$, da $\chi(d) - 1$ eine Einheit ist. Also ist $\varphi_\chi \neq \mathrm{id}_A$. □

Aufgrund dieses Lemmas operiert also die Charaktergruppe zur graduierenden Gruppe auf A als Gruppe von (homogenen) K-Algebraautomorphismen. Der zugehörige Invariantenring zu dieser Operation fällt unter schwachen Bedingungen mit dem Ring der neutralen Stufe der Graduierung zusammen.

Satz 7.10. *Es sei K ein Körper, D eine kommutative Gruppe und A eine D-graduierte kommutative K-Algebra. Zu jedem $d \in D$, $d \neq 0$, gebe es einen Charakter $\chi \in D^\vee$ mit*

$$\chi(d) \;\neq\; 1.$$

Dann ist A_0 der Invariantenring unter der natürlichen Operation der Charaktergruppe $G = D^\vee$ auf A.

Beweis. Für ein Element $f \in A_0$ und einen beliebigen Charakter χ ist offenbar

$$\varphi_\chi(f) \;=\; \chi(0)f \;=\; f,$$

so dass $A_0 \subseteq A^G$ ist. Da die Operation der Charaktergruppe homogen ist, sind die homogenen Komponenten eines invarianten Elements $f \in A^G$ ebenfalls invariant. Sei $f \in A_d \cap A^G$ und $d \neq 0$. Aufgrund der Voraussetzung gibt es einen Charakter

$$\chi\colon\ D \longrightarrow K^\times$$

mit $\chi(d) \neq 1$. Dann ist

$$\varphi_\chi(f) \ = \ \chi(d)f \ \neq \ f,$$

also sind solche Elemente nicht invariant. □

Korollar 7.11. *Es sei K ein Körper, D eine endliche kommutative Gruppe und A eine D-graduierte kommutative K-Algebra. Der Körper enthalte hinreichend viele Einheitswurzeln, so dass die Charaktergruppe $G = D^\vee$ von D isomorph zu D sei. Dann ist A_0 der Invariantenring unter der natürlichen Operation der Charaktergruppe G auf A.*

Beweis. Dies folgt direkt aus Satz 7.10. □

Beispiel 7.12. Es sei K ein Körper der positiven Charakteristik p und der Polynomring $K[X]$ sei durch $D = \mathbb{Z}/(p)$ über $\mathbb{Z} \to \mathbb{Z}/(p)$ graduiert. Die neutrale Stufe ist offenbar $K[X^p]$. Die Charaktergruppe zu $\mathbb{Z}/(p)$ ist aber trivial, da es wegen

$$(x-1)^p \ = \ x^p - 1$$

neben der 1 keine weiteren p-ten Einheitswurzeln in K gibt. Damit ist natürlich auch die induzierte Operation trivial und der Invariantenring ist $K[X]$.

Wir besprechen abschließend zwei wichtige Beispiele für Invariantenringe, die die sogenannten A- bzw. die D-Singularitäten repräsentieren.

Beispiel 7.13. Es sei K ein Körper, der eine primitive n-te Einheitswurzel ξ enthalte. Wir betrachten die Untergruppe

$$G = \left\{ \begin{pmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{pmatrix} \mid \zeta^n = 1 \right\} \subseteq \mathrm{GL}_2(K)$$

und die zugehörige Operation auf K^2 bzw. auf $K[U,V]$. Es handelt sich um eine zyklische Gruppe der Ordnung n, die von

$$g = \begin{pmatrix} \xi & 0 \\ 0 & \xi^{-1} \end{pmatrix}$$

erzeugt wird. Die Operation von g auf $K[U,V]$ ist durch $U \mapsto \xi U$ und $V \mapsto \xi^{-1}V$ gegeben. Offenbar sind

$$X = U^n,\ Y = V^n,\ Z = UV$$

invariante Polynome unter dieser Gruppenoperation, die in der Beziehung

$$XY \ = \ Z^n$$

stehen. Dass diese drei Invarianten den Invariantenring erzeugen, sieht man am besten, wenn man die Situation graduiert realisiert. Dazu sei der Polynomring $\mathbb{Z} \times \mathbb{Z}$-graduiert, wobei U den Grad $(1,0)$ und V den Grad $(0,1)$ besitze. Wir betrachten den Gruppenhomomorphismus

$$\delta\colon\ \mathbb{Z}^2 \longrightarrow \mathbb{Z}/(n) =: D,\ (a,b) \longmapsto a-b,$$

und die zugehörige D-Graduierung des Polynomringes. Wir identifizieren die Charaktergruppe $D^\vee$ mit der obigen Gruppe G, indem wir

$$\chi\colon\ D \longrightarrow K^\times$$

mit $\begin{pmatrix} \chi(1) & 0 \\ 0 & \chi(-1) \end{pmatrix}$ identifizieren. Bei dieser Identifizierung entspricht die obige explizite Operation von G auf $K[U,V]$ der natürlichen Operation der Charaktergruppe gemäß Lemma 7.9. Nach Korollar 7.11 ist der Invariantenring unter der G-Operation gleich der neutralen Stufe unter der D-Graduierung. Der Kern von δ wird durch $(n,0),(0,n),(1,1)$ erzeugt. Die zugehörigen Stufen bilden somit den Invariantenring. Der Invariantenring ist also $K[U^n,V^n,UV]$.

Im vorstehenden Beispiel haben wir einen surjektiven Ringhomomorphismus

$$K[X,Y,Z]/(XY-Z^n) \longrightarrow K[U^n,V^n,UV] = K[U,V]^G.$$

Dies ist in der Tat ein Isomorphismus, d.h. $XY = Z^n$ ist die einzige relevante Gleichung. Dies liegt daran, dass das Polynom $XY - Z^n$ irreduzibel ist und dadurch der Restklassenring $K[X,Y,Z]/(XY-Z^n)$ ein Integritätsbereich ist. Die Übereinstimmung mit dem Invariantenring folgt nun aus der Dimensionstheorie, die wir aber nicht systematisch entwickeln werden. Jedenfalls ist dieser Restklassenring und der gesuchte Invariantenring zweidimensional, so dass sie übereinstimmen müssen.

Beispiel 7.14. Es sei $m \in \mathbb{N}_+$ und es sei K ein Körper der Charakteristik $\neq 2$, der eine vierte primitive Einheitswurzel i und eine $2m$-te primitive Einheitswurzel ζ enthalte. Wir betrachten die von den Matrizen

$$A = \begin{pmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{pmatrix} \text{ und } B = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

erzeugte Untergruppe G (die man auch als BD_{2m} bezeichnet) der $\mathrm{GL}_2(K)$ mit ihrer natürlichen Operation auf $R = K[U,V]$. Es sei $H \subseteq G$ die von A erzeugte zyklische Untergruppe der Ordnung $2m$. Da G die Ordnung $4m$ besitzt, ist H ein Normalteiler in G. Daher können wir mit Hilfe von Proposition 5.1 (3) und Beispiel 7.13 den Invariantenring $K[U,V]^G$ ausrechnen. Es ist ja

$$S := = K[U,V]^H = K[U^{2m},V^{2m},UV] = K[X,Y,Z]/(XY-Z^{2m}).$$

Die Operation des nichttrivialen Elementes aus $G/H \cong \mathbb{Z}/(2)$ auf diesem Invariantenring wird durch die Operation von B auf $K[U,V]$ repräsentiert.

Sie ist also durch $U \mapsto iV$ und $V \mapsto iU$ gegeben und induziert

$$X = U^{2m} \longmapsto i^{2m}V^{2m} = \rho Y\,,$$

$$Y = V^{2m} \longmapsto i^{2m}U^{2m} = \rho X\,,$$

$$Z = UV \longmapsto i^2UV = -Z\,,$$

wobei $\rho = \pm 1$ ist, je nachdem, ob m gerade oder ungerade ist.

Durch diese Operation ist S $\mathbb{Z}/(2)$-graduiert. Bei m gerade sind

$$X + Y, Z^2, Z(X - Y)$$

invariante Polynome (bei m ungerade $X - Y, Z^2, Z(X + Y)$) und Z und $X - Y$ sind semiinvariante Polynome. Mittels $X = \frac{1}{2}(X + Y) + \frac{1}{2}(X - Y)$ und $Y = \frac{1}{2}(X + Y) - \frac{1}{2}(X - Y)$ lässt sich für jedes Monom $X^iY^jZ^k$ die homogene Zerlegung bezüglich dieser Graduierung angeben (wegen $(X-Y)^2 = (X+Y)^2 - 4Z^{2m}$ kann diese Invariante durch die anderen ausgedrückt werden). Deshalb bilden $L = X + Y$, $M = Z^2$, $N = Z(X - Y)$ ein Algebraerzeugendensystem des Invariantenringes

$$R^G \;=\; S^{\mathbb{Z}/(2)}.$$

Es besteht die Relation

$$\begin{aligned} N^2 &= Z^2(X-Y)^2 \\ &= M\left(X^2 + Y^2 - 2XY\right) \\ &= M\left(L^2 - 4XY\right) \\ &= ML^2 - 4MM^m \\ &= ML^2 - 4M^{m+1}. \end{aligned}$$

Da das Polynom

$$N^2 - ML^2 + 4M^{m+1}$$

irreduzibel ist, und der Invariantenring zweidimensional sein muss, ist

$$R^G \;\cong\; K[L, M, N]/(N^2 - ML^2 + 4M^{m+1}).$$

Unter schwachen Bedingungen an den Körper K ist dieser Ring isomorph zu

$$K[X, Y, Z]/(X^2 + YZ^2 + Z^{m+1})\,.$$

7. Arbeitsblatt

Aufwärmaufgaben

Aufgabe 7.1. Es sei R ein kommutativer Ring, D eine kommutative Gruppe und A eine D-graduierte R-Algebra. Zeige $1 \in A_0$ und folgere, dass A_0 eine R-Unteralgebra von A ist.

In den meisten der folgenden Aufgaben kann man statt mit einem Grundkörper mit einem beliebigen kommutativen Grundring arbeiten.

Aufgabe 7.2. Es sei K ein Körper, D eine kommutative Gruppe und A eine D-graduierte kommutative K-Algebra. Zeige, dass zu einem Untermonoid $M \subseteq D$ der K-Vektorraum

$$\oplus_{d \in M} A_d$$

ein Unterring von A ist.

Aufgabe 7.3. Es sei K ein Körper, D eine kommutative Gruppe und A eine D-graduierte kommutative K-Algebra, die ein Integritätsbereich sei. Zeige, dass die Menge

$$M = \{d \in D | \, A_d \neq 0\}$$

ein Untermonoid von D ist.

Vor der nächsten Aufgabe erwähnen wir die folgende Definition.

Es sei K ein Körper, D eine kommutative Gruppe und A eine D-graduierte K-Algebra. Ein K-Automorphismus

$$\varphi \colon A \longrightarrow A$$

heißt *homogen*, wenn für jedes homogene Element $a \in A_d$ gilt $\varphi(a) \in A_d$.

Aufgabe 7.4. Es sei K ein Körper, D eine kommutative Gruppe und A eine D-graduierte kommutative K-Algebra. Zeige, dass der in Lemma 7.9 zu einem Charakter $\chi \in D^\vee$ eingeführte Automorphismus

$$\varphi_\chi \colon A \longrightarrow A$$

homogen ist.

Aufgabe 7.5. Es sei D eine kommutative Gruppe und R ein kommutativer D-graduierter Ring. Es sei

$$\pi \colon D \longrightarrow E$$

ein Gruppenhomorphismus mit $F = \operatorname{kern} \pi$. Zeige folgende Aussagen.

(1) R ist in natürlicher Weise E-graduiert.
(2) Die Operation von $E^\vee$ auf R im Sinne von Lemma 7.9 stimmt mit der Operation via
$$\pi^\vee \colon E^\vee \longrightarrow D^\vee$$
überein.
(3) Die neutrale Stufe von R bezüglich der E-Graduierung ist $\bigoplus_{d\in F} R_d$. Dieser Ring ist F-graduiert und seine neutrale Stufe stimmt mit der neutralen Stufe von R in der D-Graduierung überein.
(4) Vergleiche die letzte Aussage mit Proposition 5.1.

Aufgabe 7.6. Beschreibe im Sinne von Aufgabe 7.5, wie auf dem Polynomring $R[X_1, \ldots, X_n]$ (R ein kommutativer Ring) die feine Graduierung mit der Standardgraduierung zusammenhängt.

Aufgabe 7.7. Es sei K ein Körper und V ein endlichdimensionaler K-Vektorraum. Zeige, dass es auf dem Polynomring $K[V]$ keine kanonische feine Graduierung gibt.

Aufgabe 7.8. Es sei R ein kommutativer Ring, D eine kommutative Gruppe und A eine D-graduierte kommutative R-Algebra. Es sei $\mathfrak{a} \subseteq A$ ein homogenes Ideal. Zeige, dass der Restklassenring $R/\mathfrak{a}$ ebenfalls D-graduiert ist.

Aufgabe 7.9. Wir betrachten die Gruppenoperation
$$\mathbb{K}^\times \times \mathbb{K}^2 \longrightarrow \mathbb{K}^2,\ (u, x, y) \longmapsto (ux, u^{-1}y).$$
Bestimme die Bahnen der Operation. Ist der Quotient (versehen mit der Bildtopologie) ein Hausdorff-Raum?

Aufgabe 7.10. Es sei R ein Integritätsbereich mit $2 \neq 0$ und $r \in R$ ein Element, das keine Quadratwurzel in R besitze. Zeige, dass das Polynom $X^2 - r \in R[X]$ irreduzibel ist.

Aufgabe 7.11. Es sei G die Menge der stetigen geraden Funktionen und U die Menge der stetigen ungeraden Funktionen von $\mathbb{R}$ nach $\mathbb{R}$. Zeige, dass
$$\mathrm{C}^0(\mathbb{R}, \mathbb{R}) = G \oplus U$$
eine $\mathbb{Z}/(2)$-graduierte $\mathbb{R}$-Algebra ist.

Aufgabe 7.12. Es sei R ein kommutativer Ring mit $2 \in R^\times$, auf dem die Gruppe $\mathbb{Z}/(2)$ als Gruppe von Ringautomorphismen operiere. Zeige, dass man R mit einer $\mathbb{Z}/(2)$-Graduierung versehen kann derart, dass die neutrale Stufe der Invariantenring ist.

Aufgaben zum Abgeben

Aufgabe 7.13. (4 Punkte)

Es sei K ein Körper, D eine kommutative Gruppe und A eine D-graduierte kommutative K-Algebra. Es sei

$$\varphi\colon\ A \longrightarrow A$$

ein homogener Automorphismus. Zeige, dass es einen Charakter $\chi \in D^\vee$ gibt mit $\varphi = \varphi_\chi$, wobei φ_χ der gemäß Lemma 7.9 zu χ gehörige Automorphismus ist.

Aufgabe 7.14. (4 Punkte)

Es sei K ein Körper und

$$\delta\colon\ \mathbb{Z}^2 \longrightarrow \mathbb{Z}$$

ein Gruppenhomomorphismus. Bestimme die neutrale Stufe von $K[X,Y]$ zur Graduierung, die durch $\operatorname{grad}(X_1) = \delta(e_1)$ und $\operatorname{grad}(X_2) = \delta(e_2)$ gegeben ist.

Aufgabe 7.15. (4 Punkte)

Es sei K ein Körper, D eine kommutative Gruppe und R eine kommutative D-graduierte K-Algebra. Es sei $G = D^\vee$ mit der natürlichen Operation auf R. Zeige, dass $d \in D$ einen Charakter λ auf G definiert derart, dass (unter geeigneten Voraussetzungen an D und K) die Menge der Semiinvarianten bezüglich λ gerade die d-te Stufe der Graduierung ist.

Aufgabe 7.16. (3 Punkte)

Es sei K ein Körper und $n \in \mathbb{N}$. Zeige, dass das Polynom

$$XY - Z^n$$

irreduzibel ist.

8. Vorlesung - Monoidringe

Definition 8.1. Sei M ein kommutatives (additiv geschriebenes) Monoid und R ein kommutativer Ring. Dann wird der *Monoidring* $R[M]$ wie folgt konstruiert. Als R-Modul ist

$$R[M] = \bigoplus_{m \in M} Re_m,$$

d.h. $R[M]$ ist der freie Modul mit Basis e_m, $m \in M$. Die Multiplikation wird auf den Basiselementen durch

$$e_m \cdot e_k := e_{m+k}$$

definiert und auf ganz $R[M]$ distributiv fortgesetzt. Dabei definiert das neutrale Element $0 \in M$ das neutrale Element $1 = e_0$ der Multiplikation.

Bemerkung 8.2. Ein Element in einem Monoidring lässt sich eindeutig schreiben als

$$f = \sum_{m \in \tilde{M}} a_m e_m \,,$$

wobei $\tilde{M} \subseteq M$ eine endliche Teilmenge ist und $a_m \in R$. Addiert wird komponentenweise und die Multiplikation ist explizit gegeben durch

$$f \cdot g = \left(\sum_{m \in \tilde{M}} a_m e_m \right) \left(\sum_{k \in \bar{M}} b_k e_k \right) = \sum_{\ell \in M} \left(\sum_{m+k=\ell, m \in \tilde{M}, k \in \bar{M}} a_m b_k \right) e_\ell .$$

Dies ist gemeint mit distributiver Fortsetzung. Die Menge der ℓ, über die hier summiert wird, ist endlich, und auch die inneren Summen sind jeweils endlich.

Es ist üblich, statt e_m suggestiver X^m zu schreiben, wobei X ein Symbol ist, das an eine Variable erinnern soll. Die Multiplikationsregel $X^m X^k = X^{m+k}$ erinnert dann an die entsprechende Regel für Polynomringe. In der Tat sind Polynomringe Spezialfälle von Monoidringen, und diese Notation stammt von dort. Auch ein exakter Beweis, dass in der Tat ein Ring mit assoziativer und distributiver Multiplikation vorliegt, funktioniert wie im Fall von Polynomringen. Meistens schreibt man ein Element einfach als $\sum_{m \in M} a_m X^m$, wobei fast alle $a_m = 0$ sind. Elemente der Form X^m nennt man *Monome*. Die Abbildung $M \to R[M]$, $m \mapsto X^m$, ist ein Monoidhomomorphismus, wobei rechts die multiplikative Monoidstruktur des Monoidringes genommen wird.

Ein Monoidring ist in natürlicher Weise eine R-Algebra, und zwar sind die Elemente f aus R aufgefasst in $R[M]$ gleich

$$f = f \cdot 1 = fX^0.$$

Man nennt daher auch R den *Grundring* des Monoidringes. Monoidringe sind bereits für Grundkörper interessant.

Beispiel 8.3. Sei n eine natürliche Zahl und $M = \mathbb{N}^n$ das n-fache direkte Produkt der natürlichen Zahlen. Ein Element $k \in \mathbb{N}^n$ ist also ein n-Tupel $(k_1, \ldots, k_n)$ mit $k_i \in \mathbb{N}$. Dies kann man auch als

$$(k_1, \ldots, k_n) = k_1(1, 0, 0, \ldots, 0) + k_2(0, 1, 0, \ldots, 0) + \ldots + k_n(0, 0, 0, \ldots, 1)$$

schreiben. Damit lässt sich das zugehörige Monom X^k eindeutig als

$$X^k = X_1^{k_1} X_2^{k_2} \cdots X_n^{k_n}$$

schreiben, wobei wir $X_i = X^{e_i} = X^{(0,\ldots,0,1,0,\ldots,0)}$ für das Monom zum i-ten Basiselement geschrieben haben. Das bedeutet aber, dass der Monoidring zum Monoid $\mathbb{N}^n$ über R genau der Polynomring in n Variablen ist. Insbesondere ist $R[\mathbb{N}] = R[X]$. Der Monoidring zum trivialen Monoid ist der Grundring selbst.

Beispiel 8.4. Sei n eine natürliche Zahl und $M = \mathbb{Z}^n$ das n-fache direkte Produkt der ganzen Zahlen. M ist also die freie Gruppe vom Rang n. Jedes Element $k \in \mathbb{Z}^n$ ist ein n-Tupel $(k_1, \ldots, k_n)$ mit $k_i \in \mathbb{Z}$. Dies kann man auch als

$$(k_1, \ldots, k_n) = k_1(1, 0, 0, \ldots, 0) + k_2(0, 1, 0, \ldots, 0) + \ldots + k_n(0, 0, 0, \ldots, 1)$$

schreiben und das zugehörige Monom X^k kann man eindeutig als

$$X^k = X_1^{k_1} X_2^{k_2} \cdots X_n^{k_n}$$

mit $k_i \in \mathbb{Z}$ schreiben, wobei wir wieder $X_i = X^{e_i}$ geschrieben haben. Für diesen Monoidring schreibt man auch

$$R[M] = R[X_1, \ldots, X_n, X_1^{-1}, \ldots, X_n^{-1}]\,,$$

und dieser ist isomorph zur Nenneraufnahme des Polynomringes am Produkt der Variablen, also

$$R[M] \;=\; R[X_1, \ldots, X_n, X_1^{-1}, \ldots, X_n^{-1}] \;=\; R[X_1, \ldots, X_n]_{X_1 \cdots X_n},$$

Diesen Ring nennt man auch den *Laurent-Ring* in n Variablen über R.

Universelle Eigenschaft der Monoidringe

Satz 8.5. *Sei R ein kommutativer Ring und sei M ein kommutatives Monoid. Sei B eine kommutative R-Algebra und*

$$\varphi\colon\; M \longrightarrow B$$

ein Monoidhomomorphismus (bezüglich der multiplikativen Struktur von B). Dann gibt es einen eindeutig bestimmten R-Algebrahomomorphismus

$$\tilde{\varphi}\colon\; R[M] \longrightarrow B$$

derart, dass das Diagramm

$$\begin{array}{ccc} M & \longrightarrow & R[M] \\ & \searrow & \downarrow \\ & & B \end{array}$$

kommutiert.

Beweis. Ein R-Modul-Homomorphismus $\tilde{\varphi}\colon R[M] \to B$ ist festgelegt durch die Bilder der Basiselemente X^m, $m \in M$. Das Diagramm kommutiert genau dann, wenn $\tilde{\varphi}(X^m) = \varphi(m)$ ist. Durch diese Bedingung ist die Abbildung also eindeutig festgelegt und ist bereits ein R-Modul-Homomorphismus. Es ist zu zeigen, dass dieser Homomorphismus auch die Multiplikation respektiert. Es ist $\tilde{\varphi}(1) = \tilde{\varphi}(X^0) = \varphi(0) = 1$. Ferner ist

$$\tilde{\varphi}(X^m X^k) = \tilde{\varphi}(X^{m+k}) = \varphi(m+k) = \varphi(m) \cdot \varphi(k) = \tilde{\varphi}(X^m) \cdot \tilde{\varphi}(X^k).$$

Auf der Ebene der Monome respektiert die Abbildung also die Multiplikation. Daraus folgen für zwei Elemente $f = \sum_{m \in M} a_m X^m$ und $g = \sum_{k \in M} b_k X^k$ die Identitäten

$$\begin{aligned}
\tilde{\varphi}\left(\left(\sum_{m\in M} a_m X^m\right)\left(\sum_{k\in M} b_k X^k\right)\right) &= \tilde{\varphi}\left(\sum_{\ell\in M}\left(\sum_{m+k=\ell} a_m b_k\right) X^\ell\right) \\
&= \sum_{\ell\in M}\left(\sum_{m+k=\ell} a_m b_k\right)\varphi(\ell) \\
&= \sum_{m,k\in M} a_m b_k \varphi(m)\varphi(k) \\
&= \left(\sum_{m\in M} a_m \varphi(m)\right)\left(\sum_{k\in M} b_k \varphi(k)\right) \\
&= \tilde{\varphi}\left(\sum_{m\in M} a_m X^m\right)\tilde{\varphi}\left(\sum_{k\in M} b_k X^k\right),
\end{aligned}$$

so dass die Abbildung ein Ringhomomorphismus ist. □

Korollar 8.6. *Sei R ein kommutativer Ring. Seien M und N kommutative Monoide und sei*

$$\varphi\colon M \longrightarrow N$$

ein Monoidhomomorphismus. Dann induziert dies einen R-Algebrahomomorphismus zwischen den zugehörigen Monoidringen

$$\tilde{\varphi}\colon R[M] \longrightarrow R[N],\ X^m \longmapsto X^{\varphi(m)}.$$

Beweis. Dies folgt aus Satz 17.5 (Algebraische Kurven (Osnabrück 2012)) angewandt auf die R-Algebra $B = R[N]$ und den zusammengesetzten Monoidhomomorphismus $M \xrightarrow{\varphi} N \to R[N]$. □

Bemerkung 8.7. Eine Familie von Elementen $m_i \in M$, $i \in I$, in einem Monoid M ergibt einen Monoidhomomorphismus $\mathbb{N}^{(I)} \to M$, indem das i-te Basiselement e_i auf m_i geschickt wird. Dies ist insbesondere für endliche Indexmengen $I = \{1, \ldots, n\}$ relevant. Der Monoidhomomorphismus induziert dann nach Korollar 8.6 einen R-Algebra-Homomorphismus $R[\mathbb{N}^n] = R[X_1, \ldots, X_n] \to R[M]$ von der Polynomalgebra in den Monoidring.

Diese Abbildung ist der Einsetzungshomomorphismus, der durch $X_i \mapsto X^{m_i}$ gegeben ist.

Definition 8.8. Zu einem kommutativen Monoid M und einem kommutativen Ring R nennt man einen Monoidhomorphismus

$$M \longrightarrow (R, \cdot, 1)$$

auch einen *R-wertigen Punkt* von M.

Lemma 8.9. *Sei R ein von null verschiedener kommutativer Ring. Seien M und N kommutative Monoide und sei $\varphi\colon M \to N$ ein Monoidhomomorphismus. Dann ist φ genau dann injektiv (surjektiv), wenn der zugehörige R-Algebra-Homomorphismus $\tilde{\varphi}\colon R[M] \to R[N]$ injektiv (surjektiv) ist.*

Beweis. Sei φ injektiv, und angenommen, dass

$$\tilde{\varphi}\left(\sum_{m\in M} a_m X^m\right) = \sum_{m\in M} a_m X^{\varphi(m)} = 0.$$

Da die $\varphi(m)$, $m \in M$, alle verschieden sind, folgt daraus $a_m = 0$. Ist umgekehrt φ nicht injektiv, sagen wir $\varphi(m) = \varphi(k)$, $m \neq k$, so ist auch $\tilde{\varphi}(X^m) = \tilde{\varphi}(X^k)$, obwohl $X^m \neq X^k$ ist.

Ist φ surjektiv, so kann man für ein beliebiges Element $\sum_{n\in N} a_n X^n$ aus $R[N]$ sofort ein Urbild angeben, nämlich $\sum_{n\in N} a_n X^{m_n}$, wobei m_n ein beliebiges Urbild von n sei. Ist hingegen φ nicht surjektiv, so sei $n \in N$ ein Element, das nicht zum Bild gehört. Dann ist das Monom X^n von null verschieden und kann nicht im Bild des Algebra-Homomorphismus liegen. □

Korollar 8.10. *Sei R ein von null verschiedener kommutativer Ring. Sei M ein kommutatives Monoid und $m_i \in M$, $i \in I$, eine Familie von Elementen aus M. Dann bilden die m_i genau dann ein Monoid-Erzeugendensystem für M, wenn die X^{m_i}, $i \in I$, ein R-Algebra-Erzeugendensystem für den Monoidring $R[M]$ bilden.*

Beweis. Die m_i, $i \in I$, bilden genau dann ein Monoid-Erzeugendensystem für M, wenn der Monoidhomomorphismus $\mathbb{N}^{(I)} \to M$ surjektiv ist. Dies ist nach Lemma 8.9 genau dann der Fall, wenn der zugehörige Homomorphismus

$$R[X_i, i \in I] \longrightarrow R[M],\ X_i \longmapsto X^{m_i},$$

surjektiv ist. Dies ist aber genau dann der Fall, wenn die X^{m_i} ein R-Algebra-Erzeugendensystem bilden. □

Korollar 8.11. *Sei R ein kommutativer Ring und S eine R-Algebra. Es sei M ein kommutatives Monoid. Dann gibt es einen natürlichen R-Algebra-Homomorphismus*

$$R[M] \longrightarrow S[M],\ \sum_{m\in M} a_m X^m \longmapsto \sum_{m\in M} a_m X^m,$$

(die Koeffizienten aus R werden also einfach in S aufgefasst).

Beweis. Dies folgt aus Satz 17.5 (Algebraische Kurven (Osnabrück 2012)), angewandt auf die R-Algebra $S[M]$ und den Monoidhomorphismus $M \to S[M]$. □

Differenzengruppe zu einem Monoid

Wir interessieren uns nun für die Frage, wann ein Monoidring ein Integritätsbereich ist (was nur bei integrem Grundring sein kann) und wie man dann den Quotientenkörper beschreiben kann. Da im Quotientenkörper jedes von null verschiedene Element invertierbar sein muss, gilt das insbesondere für die Monome T^m, $m \in M$, und es liegt nahe, nach einer additiven Gruppe zu suchen, die M umfasst.

Definition 8.12. Sei M ein kommutatives Monoid. Dann nennt man die Menge der *formalen Differenzen*

$$\Gamma(M) = \{m - n | \, m, n \in M\}$$

mit der Addition

$$(m_1 - n_1) + (m_2 - n_2) := (m_1 + m_2) - (n_1 + n_2)$$

und der Identifikation

$$m_1 - n_1 = m_2 - n_2 \text{ falls es } m \in M \text{ gibt mit } m + m_1 + n_2 = m + m_2 + n_1 \, .$$

die *Differenzengruppe* zu M.

Wir überlassen es dem Leser als Aufgabe, zu zeigen, dass die Differenzengruppe wirklich eine Gruppe ist. Die vorstehende Konstruktion ist natürlich der Konstruktion von Quotientenkörpern bzw. Quotientenringen nachempfunden, man muss nur die multiplikative Schreibweise dort additiv umdeuten. Die Konstruktion der Differenzengruppe ist eigentlich elementarer. Die Differenzengruppe zum additiven Monoid $\mathbb{N}$ ist natürlich $\mathbb{Z}$. Die Elemente in einem Monoid kann man direkt im Differenzenmonoid auffassen, und zwar durch den Monoidhomomorphismus

$$M \longrightarrow \Gamma(M), \, m \longmapsto m - 0 \, ,$$

wobei wir statt $m - 0$ einfach m schreiben. Völlig unproblematisch ist dieser Übergang aber doch nicht, da diese Abbildung im Allgemeinen nicht injektiv sein muss. Das hat damit zu tun, dass in der obigen Definition bei der Identifizierung links und rechts ein m auftreten darf (und das lässt sich auch nicht vermeiden). Natürlich will man auch diejenigen Monoide charakterisieren, für die man dieses Extra-m nicht braucht.

Definition 8.13. Man sagt, dass in einem kommutativen Monoid M die *Kürzungsregel* gilt (oder dass M ein *Monoid mit Kürzungsregel* ist), wenn aus einer Gleichung

$$m + n = m + k \text{ mit } m, n, k \in M \, ,$$

stets folgt, dass $n = k$ ist.

Für ein solches Monoid ist die Abbildung in die Differenzengruppe injektiv, siehe Aufgabe 8.4.

Weitere Begriffe für Monoide

Definition 8.14. Ein kommutatives Monoid M heißt *endlich erzeugt*, wenn es Elemente $m_1, \ldots, m_n \in M$ gibt derart, dass man jedes $m \in M$ als

$$m = \sum_{j=1}^{n} a_j m_j$$

mit $a_j \in \mathbb{N}$ schreiben kann.

Definition 8.15. Ein kommutatives Monoid M heißt *spitz*, wenn 0 das einzige invertierbare Element in M ist.

Definition 8.16. Ein kommutatives Monoid M heißt *torsionsfrei*, wenn für $m, n \in M$ aus $rm = rn$ für eine positive Zahl $r \in \mathbb{N}_+$ stets $m = n$ folgt.

Wenn M ein endlich erzeugtes, torsionsfreies Monoid mit Kürzungsregel ist, so ist die zugehörige Differenzengruppe isomorph zu $\mathbb{Z}^n$ und wird auch das *Differenzengitter* zu M genannt.

Definition 8.17. Sei M ein torsionsfreies kommutatives Monoid mit Kürzungsregel und mit zugehöriger Differenzengruppe $\Gamma(M)$. Dann heißt das Untermonoid

$$\tilde{M} = \{m \in \Gamma(M) |\ \text{es gibt } r \in \mathbb{N}_+ \text{ mit } rm \in M\}$$

die *Normalisierung* von M.

Ein Monoid heißt *normal*, wenn es ein torsionsfreies Monoid mit Kürzungsregel ist und mit seiner Normalisierung übereinstimmt.

8. Arbeitsblatt

Aufwärmaufgaben

Aufgabe 8.1. Seien $M \subseteq N$ kommutative Monoide. Zeige, dass durch

$$\tilde{M} = \{n \in N | \text{ es gibt } k \in \mathbb{N}_+ \text{ mit } kn \in M\}$$

ein Untermonoid von N gegeben ist, das M umfasst.

Aufgabe 8.2. Wir betrachten die kommutativen Monoide $M = \mathbb{N}^r$ und $N = \mathbb{N}^s$. Zeige, dass ein Monoidhomomorphismus von M nach N eindeutig durch eine Matrix (mit r Spalten und s Zeilen) mit Einträgen aus $\mathbb{N}$ bestimmt ist.

Aufgabe 8.3. Sei M ein kommutatives Monoid. Zeige, dass die zugehörige Differenzgruppe $\Gamma = \Gamma(M)$ eine kommutative Gruppe ist, und dass sie folgende universelle Eigenschaft besitzt: Zu jedem Monoidhomomorphismus

$$\varphi\colon\ M \longrightarrow G$$

in eine Gruppe G gibt es einen eindeutig bestimmten Gruppenhomomorphismus

$$\tilde{\varphi}\colon\ \Gamma \longrightarrow G,$$

der φ fortsetzt.

Aufgabe 8.4. Sei M ein kommutatives Monoid mit zugehöriger Differenzgruppe $\Gamma = \Gamma(M)$. Zeige, dass folgende Aussagen äquivalent sind.

(1) M ist ein Monoid mit Kürzungsregel.
(2) Die kanonische Abbildung $M \to \Gamma(M)$ ist injektiv.
(3) M lässt sich als Untermonoid einer Gruppe realisieren.

Aufgabe 8.5. Sei R ein kommutativer Ring. Beweise die R-Algebraisomorphie

$$R[\mathbb{Z}^n] \cong R[X_1, \ldots, X_n]_{X_1 \cdots X_n}$$

mit Hilfe der universellen Eigenschaften von Monoidringen und Nenneraufnahmen.

Aufgaben zum Abgeben

Aufgabe 8.6. (4 Punkte)

Es sei K ein Körper und G eine Gruppe. Dann können wir den Monoidring $K[G]$ betrachten. Sei nun weiter M ein $K[G]$-Modul. Zeige, dass

(1) M nichts anderes ist als ein K-Vektorraum V zusammen mit einem Gruppenhomomorphismus $\rho : G \to \mathrm{Aut}_K(V)$.
(2) ein $K[G]$-Modulhomomorphismus $\varphi : M \to M$ eine K-lineare Abbildung ist, für die zusätzlich $\varphi \circ \rho(g) = \rho(g) \circ \varphi$ für alle $g \in G$ gilt.

Bemerkung: ρ heißt dann eine *Darstellung* von G. Solche Darstellungen sind oft einfacher zu handhaben als G und man kann mit Hilfe von ρ oft hilfreiche Erkenntnisse über G selbst gewinnen.

9. Vorlesung - Monoidringe als Invariantenringe

In dieser Vorlesung möchten wir Monoidringe als Invariantenringe zu einer Gruppenoperation auf einem Polynomring realisieren, wobei wir den Weg über graduierte Ringe beschreiten. Wir zitieren den folgenden Satz, das sogenannte *Lemma von Gordan*, das eine Beziehung zwischen (normalen, torsionsfreien, endlich erzeugten) Monoiden (mit Kürzungsregel) und endlich erzeugten rationalen konvexen Kegeln stiftet. Ein solcher (polyedrischer) Kegel besteht aus allen Linearkombinationen mit nichtnegativen Koeffizienten zu einer endlichen Familie von Vektoren im $\mathbb{Q}^n$. Er heißt *spitz*, wenn er abgesehen vom Nullpunkt vollständig in einem Halbraum liegt. Ein solcher Kegel ist der Durchschnitt von endlich vielen Halbräumen (auch dies ist ein Satz aus der Theorie der polyedrischen Kegel).

Satz 9.1. (1) *Es sei $M \subseteq \mathbb{Z}^n$ ein normales endlich erzeugtes Monoid und $C = \mathbb{Q}_{\geq 0}M$ der zugehörige rationale Kegel. Dann ist $M = \Gamma \cap C$, wobei $\Gamma \subseteq \mathbb{Z}^n$ das Differenzengitter zu M ist.*
(2) *Wenn umgekehrt $\Gamma \subseteq \mathbb{Q}^n$ eine endlich erzeugte Untergruppe und $C \subseteq \mathbb{Q}^n$ ein endlich erzeugter rationaler Kegel ist, so ist der Durchschnitt $M = \Gamma \cap C$ ein normales endlich erzeugtes Monoid.*

Statt im $\mathbb{Q}^n$ kann man genauso gut im $\mathbb{R}^n$ arbeiten, allerdings wird verlangt, dass die Kegel von Vektoren mit rationalen Koordinaten erzeugt werden.

Normale Monoidringe als Invariantenringe

Wir betrachten auf dem Polynomring $K[X_1, \ldots, X_r]$ Graduierungen, die aus der feinen Graduierung, bei der die Variable X_i den Grad $e_i \in \mathbb{Z}^r$ bekommt,

hervorgehen, indem man einen Gruppenhomomorphismus

$$\delta\colon \mathbb{Z}^r \longrightarrow D$$

in eine kommutative Gruppe D fixiert (den man als surjektiv voraussetzen darf). Dies ergibt eine D-Graduierung des Polynomrings, bei der der Grad der Variable X_i durch

$$\delta(X_i) := \delta(e_i)$$

festgelegt ist. Die neutrale Stufe dieses so graduierten Polynomringes besteht aus den Linearkombinationen aller Monome $X_1^{a_1} \cdots X_r^{a_r}$, deren Exponententupel $(a_1, \ldots, a_r) \in \mathbb{Z}^r$ unter δ auf $0 \in D$ abgebildet wird. Die neutrale Stufe wird also durch den Kern von δ vollständig beschrieben. Wenn umgekehrt eine Untergruppe $\Delta \subseteq \mathbb{Z}^r$ gegeben ist, so kann man die Restklassenabbildung

$$\mathbb{Z}^r \longrightarrow \mathbb{Z}^r/\Delta =: D$$

betrachten und erhält so einen D-graduierten Ring.

Satz 9.2. *Es sei K ein Körper. Für eine kommutative K-Algebra R sind folgende Aussagen äquivalent.*

(1) *R ist ein K-Monoidring zu einem endlich erzeugten, torsionsfreien, normalen, spitzen Monoid mit Kürzungsregel.*
(2) *R ist die neutrale Stufe einer D-Graduierung eines Polynomringes $K[X_1, \ldots, X_r]$, wobei die Graduierung durch einen surjektiven Gruppenhomomorphismus*

$$\delta\colon \mathbb{Z}^r \longrightarrow D$$

gegeben ist.

Beweis. (1) $\Rightarrow$ (2). Sei $R = K[M]$ mit einem kommutativen Monoid M, das die angegebenen Eigenschaften erfüllt. Dann gibt es nach Satz 9.1 (1) einen reellen Raum $\mathbb{R}^n$ und einen spitzen rationalen polyedrischen Kegel $C \subset \mathbb{R}^n$ derart, dass $M = \mathbb{Z}^n \cap C$ ist (dabei kann man $\mathbb{Z}^n$ als das Differenzengitter zu M wählen). Ein solcher Kegel ist der Durchschnitt von endlich vielen Halbräumen H_j, $j = 1, \ldots, r$. Diese Halbräume kann man mit der Hilfe von linearen Abbildungen

$$\pi_j\colon \mathbb{R}^n \longrightarrow \mathbb{R}$$

durch

$$H_j = \pi_j^{-1}(\mathbb{R}_{\geq 0})$$

realisieren. Wegen der Rationalität kann man die π_j sogar als ganzzahlig, also als Abbildungen von $\mathbb{Z}^n$ nach $\mathbb{Z}$, ansetzen. Dies führt zu einem Gruppenhomomorphismus

$$\pi\colon \mathbb{Z}^n \longrightarrow \mathbb{Z}^r,$$

der injektiv ist. Wenn nämlich $\pi(w) = 0$ ist, so gehört $w \in \mathbb{Z}^n \subset \mathbb{R}^n$ zu jedem der Halbräume H_j, und das gleiche gilt für $-w$. Wegen der Spitzheit muss $w = 0$ sein. Es sei $\Delta = \pi(\mathbb{Z}^n)$ das Bild in $\mathbb{Z}^r$ und es sei

$$\delta\colon \mathbb{Z}^r \longrightarrow \mathbb{Z}^r/\Delta =: D$$

der zugehörige Restklassenhomomorphismus. Insgesamt ist

$$\begin{aligned} M &= \mathbb{Z}^n \cap C \\ &= \mathbb{Z}^n \cap \bigcap_{j=1} H_j \\ &= \{(a_1, \ldots, a_n) \in \mathbb{Z}^n \,|\, \pi_j\,(a_1, \ldots, a_n) \geq 0 \text{ für alle } j\} \\ &\cong \{(b_1, \ldots, b_r) \in \Delta \subseteq \mathbb{Z}^r \,|\, b_j \geq 0\} \\ &= \{(b_1, \ldots, b_r) \in \Delta |\ (b_1, \ldots, b_r) \in \mathbb{N}^r\} \\ &= \mathbb{N}^r \cap \Delta \\ &= \mathbb{N}^r \cap \operatorname{kern} \delta. \end{aligned}$$

Das zuletzt angegebene Monoid besteht aber aus allen Monomen in $K[X_1, \ldots, X_r]$, deren δ-Grad gleich 0 ist. Also ist

$$K[M] \cong K[\mathbb{N}^r \cap \Delta] = K[\mathbb{N}^r \cap \operatorname{kern} \delta]$$

der Ring der neutralen Stufe von $K[X_1, \ldots, X_r]$ unter der durch δ gegebenen Graduierung. (2) $\Rightarrow$ (1). Die neutrale Stufe besteht aus sämtlichen K-Linearkombinationen zu Monomen, deren Grad unter der Graduierung 0 ist. Diese Monome bilden offenbar ein Monoid, das wir M nennen. Es ist also

$$M = \Delta \cap \mathbb{N}^r$$

mit $\Delta = \operatorname{kern} \delta \cong \mathbb{Z}^r$. Der zugehörige Monoidring stimmt mit der neutralen Stufe überein. Wegen $M \subseteq \mathbb{N}^r$ ist das Monoid spitz, torsionsfrei und genügt der Kürzungsregel. Die Normalität ist ebenfalls klar. Wegen $M = \Delta \cap \mathbb{N}^r = \Delta \cap \left(\mathbb{R}^r_{\geq 0}\right)$ folgt die endliche Erzeugtheit aus Satz 9.1 (2). □

Beispiel 9.3. Sei $k \in \mathbb{N}_+$ fixiert. Wir betrachten das Monoid $M \subseteq \mathbb{Z}^2$, das durch die Vektoren

$$(0,1),\ (1,1),\ (2,1), \ldots, (k-1,1),\ (k,1)$$

erzgeut wird. Das Differenzengitter des Monoids ist der umgebende $\mathbb{Z}^2$. Das Monoid kann man auch mit einem Kegel beschreiben, und zwar mit dem durch die beiden Linearformen $\pi_1 = (1,0)$ und $\pi_2 = (-1,k)$ festgelegten Kegel C. Für die Gleichheit $M = C \cap \mathbb{Z}^2$ muss man sich klar machen, dass man jeden Gitterpunkt innerhalb des Kegels als eine additive Kombination der vorgegebenen $k+1$ Vektoren schreiben kann. Insbesondere ist somit das Monoid normal. Wir wollen dieses Monoid mit einer Graduierung im Sinne von Satz 9.2 beschreiben. Dazu fassen wir die beiden Linearformen zu einer (injektiven) Abbildung

$$\pi\colon\ \mathbb{Z}^2 \longrightarrow \mathbb{Z}^2$$

zusammen, wobei für die Standardvektoren $\pi(1,0) = (1,-1)$ und $\pi(0,1) = (0,k)$ gilt (die Bilder der erzeugenden Vektoren $(j,1)$ sind $\pi(j,1) = (j, k-j)$). Es ist also $\pi(\mathbb{Z}^2) = \Delta = \langle (1,-1), (0,k) \rangle$ und dies ist auch der Kern unter dem surjektiven Gruppenhomomorphismus

$$\delta\colon\ \mathbb{Z}^2 \longrightarrow \mathbb{Z}/(k)$$

mit

$$\delta(e_1) \,=\, \delta(e_2) \,=\, 1.$$

Die Graduierung im nächsten Beispiel kam bereits in Lemma 5.4 zum Zuge.

Beispiel 9.4. Wir betrachten die $\mathbb{Z}$-Graduierung (aufgefasst als Gruppenhomomorphismus $\mathbb{Z}^4 \to \mathbb{Z}$) auf $K[U_1, U_2, V_1, V_2]$, bei der U_1, U_2 den Grad 1 und V_1, V_2 den Grad -1 bekommen. Der Kern dieser Graduierung ist

$$\mathbb{Z}^3 \,\cong\, \Delta \,:=\, \left\langle \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} \right\rangle \,\subset\, \mathbb{Z}^4.$$

Das Monoid wird zusätzlich von $\begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}$ erzeugt. Wir berechnen die Linearformen, die im Sinne des Beweises der Rückrichtung von Satz 9.2 den Kegel im $\mathbb{R}^3$ beschreiben, der das Monoid festlegt. Diese Linearformen ergeben sich durch die vier Projektionen des $\mathbb{R}^4$ eingeschränkt auf $\mathbb{R}^3$ mit der obigen Einbettung. Dies ergibt die Linearformen

$$\pi_1 = (1,1,0),\, \pi_2 = (0,0,1),\, \pi_3 = (1,0,1),\, \pi_4 = (0,1,0)\,.$$

Die Erzeuger dieses Kegels im $\mathbb{R}^3$ sind

$$\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} -1 \\ 1 \\ 1 \end{pmatrix}\,.$$

Sie werden durch π auf die oben erwähnten Monoiderzeuger abgebildet.

Satz 9.5. *Es sei K ein algebraisch abgeschlossener Körper der Charakteristik 0. Für eine kommutative K-Algebra R sind folgende Aussagen äquivalent.*

(1) *R ist ein K-Monoidring zu einem endlich erzeugten, torsionsfreien, normalen, spitzem Monoid mit Kürzungsregel.*
(2) *R ist die neutrale Stufe einer D-Graduierung eines Polynomringes $K[X_1, \ldots, X_r]$, wobei die Graduierung durch einen surjektiven Gruppenhomomorphismus*

$$\delta\colon\, \mathbb{Z}^r \longrightarrow D$$

gegeben ist.
(3) *R ist der Invariantenring einer treuen Operation λ der Gruppe*

$$\mu_{\ell_1}(K) \times \cdots \times \mu_{\ell_a}(K) \times \left(K^\times\right)^b$$

auf dem Polynomring $K[X_1, \ldots, X_r]$ der Form

$$\lambda(t_1, \ldots, t_{a+b}, X_i) \,=\, t_1^{d_{i,1}} \cdots t_{a+b}^{d_{i,a+b}} X_i$$

(mit $d_{i,j} \in \mathbb{Z}/(\ell_j)$ für $j \le a$ und $d_{i,j} \in \mathbb{Z}$ für $j > a$).

(4) *R ist der Invariantenring zur linearen Operation der Gruppe der invertierbaren Diagonalmatrizen*

$$\left\{\begin{pmatrix} t_1^{d_{1,1}}\cdots t_{a+b}^{d_{1,a+b}} & 0 & \cdots & 0 \\ 0 & t_1^{d_{2,1}}\cdots t_{a+b}^{d_{2,a+b}} & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & t_1^{d_{r,1}}\cdots t_{a+b}^{d_{r,a+b}} \end{pmatrix} \mid t_j^{\ell_j} = 1 \text{ für } 1 \le j \le a \right\}$$

auf dem K^r (für gewisse ℓ_j für $1 \le j \le a$).

Beweis. Die Äquivalenz von (1) und (2) folgt direkt aus Satz 9.2. Von (2) nach (3). Nach dem Hauptsatz über endlich erzeugte kommutative Gruppen ist

$$D = \mathbb{Z}/(\ell_1) \times \cdots \times \mathbb{Z}/(\ell_a) \times \mathbb{Z}^b,$$

daher ist

$$G = D^\vee = \mu_{\ell_1}(K) \times \cdots \times \mu_{\ell_a}(K) \times \left(K^\times\right)^b.$$

Die zur Graduierung gemäß Lemma 7.9 gehörende Gruppenoperation der Charaktergruppe ist für $\chi \in G$ durch

$$X_i \longmapsto \chi(\delta(e_i))X_i$$

festgelegt. Mit

$$\delta(e_i) = (\delta_{i,1}, \ldots, \delta_{i,a+b})$$

und

$$\chi = (t_1, \ldots, t_{a+b})$$

(beides entsprechend der Produktzerlegung von D bzw. von $D^\vee$)ist

$$\chi(\delta(e_i))X_i = \chi(\delta_{i,1}, \ldots, \delta_{i,a+b})\, X_i = t_1^{\delta_{i,1}} \cdots t_{a+b}^{\delta_{i,a+b}} X_i.$$

Es liegt also die im Satz beschriebene Form der Operation vor. Aufgrund der Voraussetzung an den Körper sind die Bedingungen von Satz 7.10 erfüllt, also ist die neutrale Stufe der Invariantenring. Nach Lemma 7.9 ist die Operation treu. (3) nach (2). Sei die Operation mit den Daten $d_{i,j}$ gegebenen. Wir setzen

$$D := \mathbb{Z}/(\ell_1) \times \cdots \times \mathbb{Z}/(\ell_a) \times \mathbb{Z}^b$$

und definieren einen Gruppenhomorphismus $\delta\colon \mathbb{Z}^r \to D$ durch $e_i \mapsto (d_{i1}, \ldots, d_{i,a+b})$. Die Gruppenoperation der durch δ gegebenen Graduierung ist gerade die vorgegebene Operation. Diese Aussage folgt somit aus Satz 7.10. Die Äquivalenz von (3) und (4) ist klar. □

Beispiel 7.12 zeigt, dass man im vorstehenden Satz auf die Voraussetzung der Charakteristik nicht verzichten kann.

Veronese-Ringe

Definition 9.6. Es sei A eine $\mathbb{Z}$-graduierte R-Algebra und $s \in \mathbb{N}_+$. Dann nennt man

$$A^{(s)} := \oplus_{n\in\mathbb{Z}} A_{sn} \subseteq A$$

den s-ten *Veronese-Ring* von A.

Dabei handelt es sich offenbar um einen Unterring von A. Wegen $A_0 \subseteq A^{(s)}$ liegt eine R-Unteralgebra vor. Die Veroneseringe kann man selbst $\mathbb{Z}$-graduieren, indem man entweder die Graduierung direkt übernimmt (wobei dann die Stufen, deren Index kein Vielfaches von s ist, gleich 0 sind) oder aber die Graduierung als $(A^{(s)})_d := A_{sd}$ ansetzt.

Lemma 9.7. *Es sei A eine $\mathbb{Z}$-graduierte R-Algebra und $s \in \mathbb{N}_+$. Es sei vorausgesetzt, dass R eine s-te primitive Einheitswurzel enthalte. Dann ist $A^{(s)}$ der Invariantenring unter der natürlichen Operation der Charaktergruppe $(\mathbb{Z}/(s))^\vee$.*

Beweis. Wir betrachten A als $\mathbb{Z}/(s)$-graduiert durch den kanonischen Gruppenhomomorphismus $\mathbb{Z} \to \mathbb{Z}/(s)$. Dann ist der Veronese-Ring $A^{(s)}$ die 0-te Stufe von A in dieser neuen Graduierung. Daher folgt die Aussage aus Korollar 7.11. □

Lemma 9.8. *Es sei A eine $\mathbb{Z}$-graduierte R-Algebra, die von der ersten Stufe A_1 erzeugt sei. Dann wird der Veronese-Ring $A^{(s)}$ von der Stufe A_s erzeugt.*

Beweis. Es genügt zu zeigen, dass jedes homogene Element von $A^{(s)}$ von A_s erzeugt wird. Sei also $f \in A_{sd}$. Nach Voraussetzung ist $f = \sum_{\nu\in\mathbb{N}^n} r_\nu x_1^{\nu_1} \cdots x_n^{\nu_n}$ mit Elementen $x_i \in A_1$ und mit $\sum_{i=1}^n \nu_i = sd$. Diese Summe kann man in d Teilsummen aufspalten, d.h. man kann $x^\nu = x^{\mu_1} \cdots x^{\mu_d}$ schreiben, wobei die μ_j jeweils Gradtupel vom Grad s sind. □

Beispiel 9.9. Es sei K ein Körper, $R = K[X_1, \ldots, X_n]$ der Polynomring und $R^{(s)}$ der Veronese-Ring zu $s \in \mathbb{N}_+$. Nach Lemma 7.6 ist $R^{(s)} \subseteq R$ ein direkter Summand. Bei $s \geq 2$ (und $n \geq 1$) gibt es keinen Ringhomomorphismus

$$\psi\colon\ R \longrightarrow R^{(s)}$$

mit $\psi \circ \iota = \mathrm{id}_{R^{(s)}}$. Dies liegt daran, dass

$$\psi(X_1) \ = \ a_0 + a_s + a_{2s} + \ldots + a_{rs} \ = \ X_1$$

mit $a_{is} \in R_{is}$ keine Lösung besitzt.

Veronese-Ringe zu Polynomringen

Wir betrachten nun genauer die Veronese-Ringe zum Polynomring mit der Standardgraduierung.

Lemma 9.10. *Es sei K ein Körper und $R = K[X_1, \ldots, X_n]$ der Polynomring über K in n Variablen und $s \in \mathbb{N}_+$. Dann ist der Veronese-Ring $R^{(s)}$ der Monoidring zum Monoid*

$$M = \left\{ m = (m_1, \ldots, m_n) \in \mathbb{N}^n | \sum_{i=1}^{n} m_i \in \mathbb{N}s \right\} \subseteq \mathbb{N}^n.$$

Wenn K eine s-te primitive Einheitswurzel enthält, so ist dies zugleich der Invariantenring zur linearen Operation der $\mu_s(K)$ auf dem K^n durch skalare Multiplikation.

Beweis. Dies folgt aus Satz 9.2 zur $D := \mathbb{Z}/(s)-$Graduierung

$$\mathbb{Z}^n \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Z}/(s)\,.$$

Der Kern dieser Abbildung geschnitten mit $\mathbb{N}^n$ bildet gerade die angegebene Menge. Der Zusatz folgt aus Lemma 9.7. □

Die in der letzten Aussage angesprochene Gruppenoperation ist besonders einfach, sie wird linear durch Diagonalmatrizen mit konstanten Einträgen realisiert, die s-te Einheitswurzeln sind. Die Determinanten dieser Matrizen sind i.A. nicht 1, d.h. es handelt sich nicht um eine Untergruppe der speziellen linearen Gruppe. Damit hängt der Umstand zusammen, dass die Veronese-Ringe typischerweise ziemlich viele Gleichungen benötigen, um sie als Restklassenring eines Polynomrings zu beschreiben.

Beispiel 9.11. Zum Polynomring $K[X]$ über einem Körper K und jedem $s \in \mathbb{N}_+$ ist der s-te Veronese-Ring isomorph zum Polynomring selbst. Es handelt sich einfach um den von X^s über K erzeugten Unterring.

Beispiel 9.12. Zum Polynomring $A = K[X, Y]$ über einem Körper K und einem $s \in \mathbb{N}_+$ wird der s-te Veronese-Ring durch die Monome $X^s, X^{s-1}Y, \ldots, XY^{s-1}, Y^s$ erzeugt. Bei $s = 2$ handelt es sich um

$$K[X^2, XY, Y^2] \cong K[U, V, W]/(UW - V^2)\,.$$

Bei $s = 3$ handelt es sich um

$$K[X^3, X^2Y, XY^2, Y^3] \cong K[U, V, W, Z]/(UZ - VW, UW - V^2, VZ - W^2)\,.$$

Diese Ringe sind nicht isomorph zum Polynomring in zwei Variablen. Beispielsweise ist $A^{(2)}$ im Gegensatz zum Polynomring nicht faktoriell, die Elemente U, V, W sind irreduzibel, aber nicht prim, und die Gleichung $UW = V^2$ bedeutet, dass zwei wesentlich verschiedene Zerlegungen dieses Elementes vorliegen.

9. Arbeitsblatt

Aufwärmaufgabe

Aufgabe 9.1. Beschreibe

$$K[X,Y,Z]/(XY-Z^n)$$

als Monoidring und als neutrale Stufe eines Polynomrings in einer geeigneten Graduierung.

Aufgabe 9.2. Bestimme das Monoid und den Monoidring, das durch den Kegel

$$C = \{av+bw | \, a,b \in \mathbb{R}_{\geq 0}\}$$

mit $v = \begin{pmatrix} 3 \\ 2 \end{pmatrix}$ und $w = \begin{pmatrix} 2 \\ 5 \end{pmatrix}$ bestimmt ist. Finde eine Graduierung auf $K[X,Y]$ derart, dass der Monoidring der Ring der neutralen Stufe ist.

Aufgabe 9.3. Es sei $M \subseteq \Gamma = \mathbb{Z}^n$ ein normales, spitzes Monoid, wobei Γ das Differenzengitter zu M sei. Es sei $C = \mathbb{R}_{\geq} M \subseteq \mathbb{R}^n$ der zugehörige rationale Kegel. Zeige, dass bei $n=2$ dieser Kegel durch zwei Halbräume (bzw. Linearformen) beschreibbar ist, und dass bei $n=3$ jede Anzahl an Halbräumen $r \geq n$ auftreten kann.

Die beiden nächsten Aufgaben machen zwei Extremfälle von Satz 9.5 (4) explizit.

Aufgabe 9.4. Es sei K ein Körper und $d_1, \ldots, d_r$ seien ganze Zahlen. Zeige, dass die Zuordnung

$$\mu_\ell(K) \longrightarrow \mathrm{GL}_r(K), \, t \longmapsto \begin{pmatrix} t^{d_1} & 0 & \cdots & \cdots & 0 \\ 0 & t^{d_2} & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & t^{d_{r-1}} & 0 \\ 0 & \cdots & \cdots & 0 & t^{d_r} \end{pmatrix},$$

ein Gruppenhomomorphismus ist.

Aufgabe 9.5. Es sei K ein Körper und seien $\ell_1, \ldots, \ell_a$ natürliche Zahlen und $d_1, \ldots, d_{a+b}$ ganze Zahlen. Zeige, dass die Zuordnung

$$\mu_{\ell_1}(K) \times \cdots \times \mu_{\ell_a}(K) \times \left(K^\times\right)^b \longrightarrow \mathrm{GL}_1(K) \cong K^\times,$$
$$(t_1, \ldots, t_{a+b}) \longmapsto t_1^{d_1} \cdots t_{a+b}^{d_{a+b}},$$

ein Gruppenhomomorphismus ist.

Aufgabe 9.6. Bestimme zur durch einen Gruppenhomomorphismus

$$\delta\colon\ \mathbb{Z}^2 \longrightarrow \mathbb{Z}/(3)$$

bestimmten $\mathbb{Z}/(3)$-Graduierung auf $K[U,V]$ den Ring der neutralen Stufe in Abhängigkeit von δ.

Aufgabe 9.7. Es sei K ein Körper und A eine $\mathbb{Z}$-graduierte K-Algebra, auf der eine Gruppe G als Gruppe von homogenen K-Algebrahomomorphismen operiere. Zeige

$$\left(A^{(s)}\right)^G \ = \ \left(A^G\right)^{(s)}.$$

Aufgabe 9.8. Zeige, dass der Veronese-Ring $K[U,V]^{(s)}$ als K-Algebra durch $s+1$ Elemente $Z_0, Z_1, \ldots, Z_s$ erzeugt wird derart, dass sämtliche 2×2-Minoren der Matrix

$$\begin{pmatrix} Z_0 & Z_1 & \ldots & Z_{s-2} & Z_{s-1} \\ Z_1 & Z_2 & \ldots & Z_{s-1} & Z_s \end{pmatrix}$$

Relationen zwischen diesen Erzeugern sind.

Aufgaben zum Abgeben

Aufgabe 9.9. (2 Punkte)

Es sei $A = \bigoplus_{d\in D} A_d$ ein graduierter kommutativer Ring und es sei A_e eine Stufe, die eine Einheit enthalte. Zeige, dass A_e als A_0-Modul isomorph zu A_0 ist.

Aufgabe 9.10. (3 Punkte)

Man gebe ein Beispiel eines Untermonoids $M \subseteq \mathbb{N}^2$, das nicht endlich erzeugt ist.

Aufgabe 9.11. (3 Punkte)

Es sei K ein algebraisch abgeschlossener Körper der Charakteristik 0. Bestimme in der Situation von Aufgabe 9.5 den Invariantenring der zugehörigen Operation auf dem Polynomring.

Aufgabe 9.12. (3 Punkte)

Bestimme die minimale Anzahl eines Erzeugendensystems für den Veronese-Ring $K[X_1, \ldots, X_n]^{(s)}$.

10. Vorlesung - Noethersche Ringe

Noethersche Ringe

Unser Ziel ist es zu zeigen, dass wenn R ein noetherscher Ring ist, dass dann auch der Polynomring $R[X]$ ein noetherscher Ring ist (Hilbertscher Basissatz). Dies gilt dann auch für die Hinzunahme von mehreren (endlich vielen) Variablen und insbesondere für Polynomringe in endlich vielen Variablen über einem Körper. Wir erinnern an den Begriff des noetherschen Ringes.

Emmy Noether (1882-1935)

Definition 10.1. Ein kommutativer Ring R heißt *noethersch*, wenn jedes Ideal darin endlich erzeugt ist.

Proposition 10.2. *Für einen kommutativen Ring R sind folgende Aussagen äquivalent.*

(1) *R ist noethersch.*
(2) *Jede aufsteigende Idealkette*

$$\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \mathfrak{a}_3 \subseteq \dots$$

wird stationär*, d.h. es gibt ein n mit $\mathfrak{a}_n = \mathfrak{a}_{n+1} = \dots$.*

Beweis. (1) $\Rightarrow$ (2). Sei

$$\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \mathfrak{a}_3 \subseteq \dots$$

eine aufsteigende Idealkette in R. Wir betrachten die Vereinigung $\mathfrak{a} = \bigcup_{n\in\mathbb{N}} \mathfrak{a}_n$, die wieder ein Ideal in R ist. Da R noethersch ist, ist $\mathfrak{a}$ endlich erzeugt, d.h. $\mathfrak{a} = (f_1, \dots, f_k)$. Da diese f_i in der Vereinigung der Ideale $\mathfrak{a}_n$ liegen, und

da die Ideale aufsteigend sind, muss es ein n geben derart, dass $f_1, \ldots, f_k \in \mathfrak{a}_n$ liegt. Wegen

$$(f_1, \ldots, f_k) \subseteq \mathfrak{a}_n \subseteq \mathfrak{a}_{n+m} \subseteq \bigcup_{n \in \mathbb{N}} \mathfrak{a}_n \subseteq (f_1, \ldots, f_k)$$

für $m \geq 0$ muss hier Gleichheit gelten, so dass die Idealkette ab n stationär ist.

(2) $\Rightarrow$ (1). Sei $\mathfrak{a}$ ein Ideal in R. Wir nehmen an, $\mathfrak{a}$ sei nicht endlich erzeugt, und konstruieren sukzessive eine unendliche echt aufsteigende Idealkette $\mathfrak{a}_n \subset \mathfrak{a}$, wobei die $\mathfrak{a}_n$ alle endlich erzeugt sind. Sei dazu

$$\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \ldots \subset \mathfrak{a}_n \subseteq \mathfrak{a}$$

bereits konstruiert. Da $\mathfrak{a}_n$ endlich erzeugt ist, aber $\mathfrak{a}$ nicht, ist die Inklusion $\mathfrak{a}_n \subseteq \mathfrak{a}$ echt und es gibt ein Element

$$f_{n+1} \in \mathfrak{a},\ f_{n+1} \notin \mathfrak{a}_n\,.$$

Dann setzt das Ideal $\mathfrak{a}_{n+1} := \mathfrak{a}_n + (f_{n+1})$ die Idealkette echt aufsteigend fort. □

Lemma 10.3. *Sei R ein noetherscher Ring. Dann ist auch jeder Restklassenring $R/\mathfrak{b}$ noethersch.*

Beweis. Sei $\mathfrak{a} \subseteq R/\mathfrak{b}$ ein Ideal und sei $\tilde{\mathfrak{a}} \subseteq R$ das Urbildideal davon. Dieses ist endlich erzeugt nach Voraussetzung, also $\tilde{\mathfrak{a}} = (f_1, \ldots, f_n)$. Die Restklassen dieser Erzeuger, also $\bar{f}_1, \ldots, \bar{f}_n$, bilden ein Idealerzeugendensystem von $\mathfrak{a}$: Für ein Element $\bar{g} \in \mathfrak{a}$ gilt ja $g = \sum_{i=1}^n r_i f_i$ in R und damit $\bar{g} = \sum_{i=1}^n \bar{r}_i \bar{f}_i$ in $R/\mathfrak{b}$. □

Der Hilbertsche Basissatz

Wie viele grundlegende Aussagen der kommutativen Algebra geht der Hilbertsche Basissatz, dem wir uns jetzt zuwenden, auf David Hilbert zurück, genauer auf seine Arbeit von 1890, „Ueber die Theorie der algebraischen Formen“.

David Hilbert (1862-1943)

Satz 10.4. *Sei R ein noetherscher Ring. Dann ist auch der Polynomring $R[X]$ noethersch.*

Beweis. Sei $\mathfrak{b}$ ein Ideal im Polynomring $R[X]$. Zu $n \in \mathbb{N}$ definieren wir ein Ideal $\mathfrak{a}_n$ in R durch

$$\mathfrak{a}_n = \left\{ c \in R | \text{ es gibt } F \in \mathfrak{b} \text{ mit } F = cX^n + c_{n-1}X^{n-1} + \ldots + c_1X + c_0 \right\} .$$

Das Menge $\mathfrak{a}_n$ besteht also aus allen Leitkoeffizienten von Polynomen vom Grad n aus $\mathfrak{b}$. Es handelt sich dabei offensichtlich um Ideale in R (wobei wir hier 0 als Leitkoeffizient zulassen). Ferner ist $\mathfrak{a}_n \subseteq \mathfrak{a}_{n+1}$, da man ja ein Polynom F vom Grad n mit Leitkoeffizient c mit der Variablen X multiplizieren kann, um ein Polynom vom Grad $n+1$ zu erhalten, das wieder c als Leitkoeffizienten besitzt. Da R noethersch ist, muss diese aufsteigende Idealkette stationär werden; sei n so, dass $\mathfrak{a}_n = \mathfrak{a}_{n+1} = \ldots$ ist.

Zu jedem $i \leq n$ sei nun $\mathfrak{a}_i = (c_{i1}, \ldots, c_{ik_i})$ ein endliches Erzeugendensystem, und es seien

$$F_{ij} = c_{ij}X^i + \text{ Terme von kleinerem Grad}$$

zugehörige Polynome aus $\mathfrak{b}$ (die es nach Definition der $\mathfrak{a}_i$ geben muss).

Wir behaupten, dass $\mathfrak{b}$ von allen $\{F_{ij} | \, 0 \leq i \leq n, \, 1 \leq j \leq k_i\}$ erzeugt wird. Dazu beweisen wir für jedes $G \in \mathfrak{b}$ durch Induktion über den Grad von G, dass es als Linearkombination mit diesen F_{ij} darstellbar ist. Für G konstant, also $G \in R$, ist dies klar. Sei nun der Grad von G gleich d und die Aussage sei für kleineren Grad bewiesen. Wir schreiben

$$G = cX^d + c_{d-1}X^{d-1} + \ldots + c_1X + c_0 \, .$$

Es ist $c \in \mathfrak{a}_d$ und damit kann man c schreiben als R-Linearkombination der $c_{ij}, 0 \leq i \leq n$, $1 \leq j \leq k_i$. Bei $d \leq n$ kann man c sogar schreiben als R-Linearkombination der c_{dj}, $j = 1, \ldots, k_d$, sagen wir $c = \sum_{j=1}^{k_d} r_j c_{dj}$. Dann ist $G - \sum_{j=1}^{k_d} r_j F_{dj} \in \mathfrak{b}$ und hat einen kleineren Grad, sodass man darauf die Induktionsvoraussetzung anwenden kann. Bei $d > n$ ist

$$c = \sum_{i=0,\ldots,n,\, j=1,\ldots,k_i} r_{ij} c_{ij} \, .$$

Damit gehört

$$G - \sum_{i=0,\ldots,n,\, j=1,\ldots,k_i} r_{ij} X^{d-i} F_{ij}$$

ebenfalls zu $\mathfrak{b}$ und hat einen kleineren Grad, so dass man wieder die Induktionsvoraussetzung anwenden kann. □

Korollar 10.5. *Sei R ein noetherscher Ring. Dann ist auch $R[X_1, \ldots, X_n]$ noethersch.*

Beweis. Dies folgt durch induktive Anwendung des Hilbertschen Basissatzes auf die Kette

$$\begin{aligned} R \subset R[X_1] \subset (R[X_1])[X_2] = R[X_1, X_2] \\ \subset (R[X_1, X_2])[X_3] = R[X_1, X_2, X_3] \subset \ldots \subset R[X_1, \ldots, X_n]. \end{aligned}$$

□

Korollar 10.6. *Sei K ein Körper. Dann ist $K[X_1, \ldots, X_n]$ noethersch.*

Beweis. Dies ist ein Spezialfall von Korollar 10.5. □

Definition 10.7. Es sei R ein kommutativer Ring. Eine R-Algebra A heißt *von endlichem Typ* (oder *endlich erzeugt*), wenn sie die Form

$$A = R[X_1, \ldots, X_n]/\mathfrak{a}$$

besitzt.

Eine endlich erzeugte R-Algebra besitzt also eine Darstellung als Restklassenring einer Polynomalgebra über R in endlich vielen Variablen. Eine solche Darstellung ist keineswegs eindeutig.

Korollar 10.8. *Sei R ein noetherscher Ring. Dann ist jede R- Algebra von endlichem Typ ebenfalls noethersch. Insbesondere ist für einen Körper K jede K-Algebra von endlichem Typ noethersch.*

Beweis. Dies folgt aus Korollar 10.5 und aus Lemma 10.3. □

Noethersche Moduln

Definition 10.9. Sei R ein kommutativer Ring und M ein R-Modul. Der Modul M heißt *endlich erzeugt* oder *endlich*, wenn es ein endliches Erzeugendensystem v_i, $i \in I$, für ihn gibt (also mit einer endlichen Indexmenge).

Wir wollen zeigen, das für einen noetherschen Ring R und einen endlich erzeugten R-Modul jeder R-Untermodul wieder endlich erzeugt ist. Solche Moduln nennt man noethersch.

Definition 10.10. Sei R ein kommutativer Ring und M ein R-Modul. Dann heißt M *noethersch*, wenn jeder R-Untermodul von M endlich erzeugt ist.

Für $M = R$ stimmt dies mit der Definition eines noetherschen Ringes überein, da ja die R-Untermoduln von R gerade die Ideale sind.

In den folgenden Aussagen verwenden wir folgende Sprech- bzw. Schreibweise.

Definition 10.11. Sei R ein kommutativer Ring und seien M_1, M_2, M_3 R-Moduln. Man nennt ein Diagramm der Form

$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0$$

eine *kurze exakte Sequenz* von R-Moduln, wenn M_1 ein R-Untermodul von M_2 ist, und wenn M_3 ein Restklassenmodul von M_2 ist, der isomorph zu M_2/M_1 ist.

Lemma 10.12. *Sei R ein kommutativer Ring und*

$$0 \longrightarrow M_1 \longrightarrow M \longrightarrow M_3 \longrightarrow 0$$

eine kurze exakte Sequenz von R-Moduln. Dann ist M genau dann noethersch, wenn sowohl M_1 als auch M_3 noethersch sind.

Beweis. Sei zunächst M noethersch, und $U \subseteq M_1$ ein Untermodul. Dann ist U direkt auch ein Untermodul von M, also nach Voraussetzung endlich erzeugt. Sei nun $V \subseteq M_3$ ein Untermodul des Restklassenmoduls. Das Urbild von V in M unter der Restklassenabbildung sei $\tilde{V}$. Dieser Modul ist nach Voraussetzung endlich erzeugt, und die Bilder eines solchen Erzeugendensystems erzeugen auch den Bildmodul V.

Seien nun die äußeren Moduln M_1 und M_3 noethersch, und sei $U \subseteq M$ ein Untermodul. Es sei $U_3 \subseteq M_3$ der Bild-Untermodul davon. U_3 wird von endlich vielen Elementen $s_1, \ldots, s_n$ erzeugt, und wir können annehmen, dass diese $s_i = \overline{r}_i$ die Bilder von Elementen $r_i \in U$ sind. Betrachte $U \cap M_1$. Dies ist ein Untermodul von M_1, und daher endlich erzeugt, sagen wir von $t_1, \ldots, t_k$, die wir als Elemente in U auffassen. Wir behaupten, dass

$$r_1, \ldots, r_n, t_1, \ldots, t_k$$

ein Erzeugendensystem von U bilden. Sei dazu $m \in U$ ein beliebiges Element. Dann ist $\overline{m} = \sum_{i=1}^{n} a_i s_i$ und daher geht das Element $m - \sum_{i=1}^{n} a_i r_i$ rechts auf null. Dann gehört es aber zum Kern der Restklassenabbildung, also zu M_1. Andererseits gehört dieses Element auch zu U, also zum Durchschnitt $M_1 \cap U$, der ja von den $t_1, \ldots, t_k$ erzeugt wird. Also kann man schreiben

$$m - \sum_{i=1}^{n} a_i r_i = \sum_{j=1}^{k} b_j t_j$$

bzw. $m = \sum_{i=1}^{n} a_i r_i + \sum_{j=1}^{k} b_j t_j$. □

Satz 10.13. *Sei R ein noetherscher kommutativer Ring und M ein endlich erzeugter R-Modul. Dann ist M ein noetherscher Modul.*

Beweis. Wir beweisen die Aussage durch Induktion über die Anzahl n der Modulerzeuger von M. Bei $n = 0$ liegt der Nullmodul vor. Sei $n = 1$. Dann gibt es eine surjektive Abbildung $R \to M \cong R/\mathfrak{a}$. Nach Lemma 10.12 ist aber ein Restklassenmodul eines noetherschen Moduls wieder noethersch, und der Ring selbst ist nach Voraussetzung noethersch, also ist M noethersch.

Sei nun $n \geq 2$ und die Aussage für kleinere n bereits bewiesen. Sei $m_1, \ldots, m_n$ ein Erzeugendensystem von M. Wir betrachten den durch $m_1, \ldots, m_{n-1}$ erzeugten R-Untermodul, den wir mit M_1 bezeichnen. Dieser Untermodul gibt Anlass zu einer kurzen exakten Sequenz, nämlich

$$0 \longrightarrow M_1 \longrightarrow M \longrightarrow M/M_1 =: M_3 \longrightarrow 0\,.$$

Hier wird der linke Modul von $n-1$ Elementen erzeugt und ist nach Induktionsvoraussetzung noethersch. Der rechte Modul wird von der Restklasse von m_n, also von einem Element erzeugt, ist also auch noethersch. Nach Lemma 10.12 ist dann M noethersch. □

10. Arbeitsblatt

Aufwärmaufgaben

Aufgabe 10.1. Begründe, warum der Ring

$$\mathbb{Z}[X, Y, Z, W]/(XY - ZW, 5X^8 - YZ^3 + 2WXY)$$

noethersch ist.

Aufgabe 10.2. Sei R ein kommutativer Ring und sei

$$\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \mathfrak{a}_3 \subseteq \ldots$$

eine aufsteigende Kette von Idealen. Zeige, dass die Vereinigung $\bigcup_{n\in\mathbb{N}} \mathfrak{a}_n$ ebenfalls ein Ideal ist. Zeige ebenso durch ein einfaches Beispiel, dass die Vereinigung von Idealen im Allgemeinen kein Ideal sein muss.

Aufgabe 10.3. Sei K ein Körper und sei

$$K[X_n,\, n \in \mathbb{N}]$$

der Polynomring über K in unendlich vielen Variablen. Man beschreibe darin ein nicht endlich erzeugtes Ideal und eine unendliche, echt aufsteigende Idealkette.

Vor der nächsten Aufgabe erinnern wir an die Reduktion.

Sei R ein kommutativer Ring und n_R das Nilideal von R, das aus allen nilpotenten Elementen von R besteht. Dann nennt man den Restklassenring R/n_R die *Reduktion* von R.

Aufgabe 10.4. Man gebe ein Beispiel eines nicht-noetherschen Ringes, dessen Reduktion ein Körper ist.

Aufgabe 10.5. Sei K ein Körper und sei A eine kommutative K-Algebra, die als K-Modul endlich sei. Zeige, dass ein Element $f \in A$ genau dann eine Einheit ist, wenn es ein Nichtnullteiler ist.

Aufgabe 10.6. Seien K und L Körper, sei $K \subseteq L$ eine endliche Körpererweiterung und sei A, $K \subseteq A \subseteq L$, ein Zwischenring. Zeige, dass dann A ebenfalls ein Körper ist.

Aufgabe 10.7. Es sei R ein kommutativer Ring und M ein R-Modul. Dann ist M genau dann noethersch, wenn jede aufsteigende Kette

$$M_0 \subseteq M_1 \subseteq M_2 \subseteq \ldots$$

von R-Untermoduln stationär wird.

Die folgenden Aufgaben verwenden den Begriff des artinschen Moduls, der „dual“ zum Begriff des noetherschen Moduls ist.

Sei R ein kommutativer Ring. Ein R-Modul M heißt *artinsch*, wenn jede absteigende Kette

$$M_1 \supseteq M_2 \supseteq M_3 \supseteq \ldots$$

von R-Untermoduln stationär wird.

Ein kommutativer Ring R heißt *artinsch*, wenn er als R-Modul artinsch ist.

Aufgabe 10.8. Es sei A ein artinscher Integritätsbereich. Man zeige, dass A ein Körper ist. Man gebe ein Beispiel eines artinschen kommutativen Ringes, der kein Körper ist.

Aufgabe 10.9. Sei $\mathfrak{a}$ ein Radikal in einem kommutativen Ring. Zeige, dass $\mathfrak{a}$ der Durchschnitt von Primidealen ist.

Aufgaben zum Abgeben

Aufgabe 10.10. (4 Punkte)

Sei R ein kommutativer Ring und sei I ein Ideal mit dem Restklassenring $S = R/I$. Zeige, dass die Ideale von S eindeutig denjenigen Idealen von R entsprechen, die I umfassen.

Zeige, dass das Gleiche für Primideale, Radikalideale und maximale Ideale gilt.

Aufgabe 10.11. (4 Punkte)

Zeige, dass $\mathbb{Q}$ keine Algebra von endlichem Typ über $\mathbb{Z}$ ist.

Aufgabe 10.12. (4 Punkte)

Sei K ein Körper und sei $A = K[X, Y]$. Finde eine K-Unteralgebra von A, die nicht endlich erzeugt ist.

Aufgabe 10.13. (4 Punkte)

Bestimme zum Ideal

$$I = (10, 6x^2 + 8, 4x^3 - 12)$$

in $\mathbb{Z}[x]$ die im Beweis zum Hilbertschen Basissatz konstruierte Idealkette und das zugehörige Erzeugendensystem von I. Schreibe die obigen Erzeuger als Linearkombination mit dem konstruierten Erzeugendensystem.

Aufgabe 10.14. (4 Punkte)

Sei R ein noetherscher Integritätsbereich. Zeige, dass sich jedes Element aus R als ein Produkt von irreduziblen Elementen schreiben lässt.

Aufgabe 10.15. (5 Punkte)

Sei A ein kommutativer Ring und sei

$$0 \longrightarrow M \longrightarrow N \longrightarrow P \longrightarrow 0$$

eine kurze exakte Sequenz von A-Moduln. Man zeige, dass N genau dann artinsch ist, wenn M und P artinsch sind.

Aufgabe 10.16. (4 Punkte)

Sei R ein kommutativer Ring und M ein R-Modul. Zeige: Wenn M artinsch und $\phi : M \to M$ R-linear und injektiv ist, so ist ϕ ein Isomorphismus. Formuliere und beweise auch eine analoge Aussage für den Fall, das M noethersch ist.

11. Vorlesung - Ganzheit

Ganzheit

In der nächsten Vorlesung werden wir sehen, dass bei einer endlichen Gruppe, die auf einem kommutativen Ring als Gruppe von Ringautomorphismen operiert, der Ring ganz über seinem Invariantenring ist, wodurch eine enge Beziehung zwischen diesen beiden Ringen gestiftet wird. Hier führen wir die Ganzheit und verwandte Begriffe ein.

Definition 11.1. Seien R und S kommutative Ringe und $R \subseteq S$ eine Ringerweiterung. Für ein Element $x \in S$ heißt eine Gleichung der Form

$$x^n + r_{n-1}x^{n-1} + r_{n-2}x^{n-2} + \ldots + r_1 x + r_0 = 0,$$

wobei die Koeffizienten r_i, $i = 0, \ldots, n-1$, zu R gehören, eine *Ganzheitsgleichung* für x.

Definition 11.2. Seien R und S kommutative Ringe und $R \subseteq S$ eine Ringerweiterung. Ein Element $x \in S$ heißt *ganz*, wenn x eine Ganzheitsgleichung mit Koeffizienten aus R erfüllt.

Definition 11.3. Seien R und S kommutative Ringe und $R \subseteq S$ eine Ringerweiterung. Dann nennt man die Menge der Elemente $x \in S$, die ganz über R sind, den *ganzen Abschluss* von R in S.

Definition 11.4. Seien R und S kommutative Ringe und $R \subseteq S$ eine Ringerweiterung. Dann heißt S *ganz* über R, wenn jedes Element $x \in S$ ganz über R ist.

S ist genau dann ganz über R, wenn der ganze Abschluss von R in S gleich S ist.

Lemma 11.5. *Seien R und S kommutative Ringe und $R \subseteq S$ eine Ringerweiterung. Für ein Element $x \in S$ sind folgende Aussagen äquivalent.*

(1) *x ist ganz über R.*
(2) *Es gibt eine R-Unteralgebra T von S mit $x \in T$ und die ein endlicher R-Modul ist.*
(3) *Es gibt einen endlichen R-Untermodul M von S, der einen Nichtnullteiler aus S enthält, mit $xM \subseteq M$.*

Beweis. (1) $\Rightarrow$ (2). Wir betrachten die von den Potenzen von x erzeugte R-Unteralgebra $R[x]$ von S, die aus allen polynomialen Ausdrücken in x mit Koeffizienten aus R besteht. Aus einer Ganzheitsgleichung

$$x^n + r_{n-1}x^{n-1} + r_{n-2}x^{n-2} + \ldots + r_1 x + r_0 = 0$$

ergibt sich

$$x^n = -r_{n-1}x^{n-1} - r_{n-2}x^{n-2} - \ldots - r_1 x - r_0\,.$$

Man kann also x^n durch einen polynomialen Ausdruck von einem kleineren Grad ausdrücken. Durch Multiplikation dieser letzten Gleichung mit x^i kann man jede Potenz von x mit einem Exponenten $\geq n$ durch einen polynomialen Ausdruck von einem kleineren Grad ersetzen. Insgesamt kann man dann aber all diese Potenzen durch polynomiale Ausdrücke vom Grad $\leq n-1$ ersetzen. Damit ist

$$R[x] = R + Rx + Rx^2 + \ldots + Rx^{n-2} + Rx^{n-1}$$

und die Potenzen $x^0 = 1, x^1, x^2, \ldots, x^{n-1}$ bilden ein endliches Erzeugendensystem von $T = R[x]$.

(2) $\Rightarrow$ (3). Sei $x \in T \subseteq S$, T eine R-Unteralgebra, die als R-Modul endlich erzeugt sei. Dann ist $xT \subseteq T$, und T enthält den Nichtnullteiler 1.

(3) $\Rightarrow$ (1). Sei $M \subseteq S$ ein endlich erzeugter R-Untermodul mit $xM \subseteq M$. Seien $y_1, \ldots, y_n$ erzeugende Elemente von M. Dann ist insbesondere xy_i für jedes i eine R-Linearkombination der y_j, $j = 1, \ldots, n$. Dies bedeutet

$$xy_i = \sum_{j=1}^{n} r_{ij} y_j$$

mit $r_{ij} \in R$ oder als Matrix geschrieben

$$x \begin{pmatrix} y_1 \\ y_2 \\ . \\ . \\ y_n \end{pmatrix} = \begin{pmatrix} r_{1,1} & r_{1,2} & . & . & r_{1,n} \\ r_{2,1} & r_{2,2} & . & . & r_{2,n} \\ . & . & . & . & . \\ . & . & . & . & . \\ r_{n,1} & r_{n,2} & . & . & r_{n,n} \end{pmatrix} \cdot \begin{pmatrix} y_1 \\ y_2 \\ . \\ . \\ y_n \end{pmatrix} .$$

Dies schreiben wir als

$$0 = \begin{pmatrix} x - r_{1,1} & -r_{1,2} & . & . & -r_{1,n} \\ -r_{2,1} & x - r_{2,2} & . & . & -r_{2,n} \\ . & . & . & . & . \\ . & . & . & . & . \\ -r_{n,1} & -r_{n,2} & . & . & x - r_{n,n} \end{pmatrix} \cdot \begin{pmatrix} y_1 \\ y_2 \\ . \\ . \\ y_n \end{pmatrix} .$$

Nennen wir diese Matrix A (die Einträge sind aus S), und sei A^{adj} die adjungierte Matrix. Dann gilt $A^{adj}Ay = 0$ (y bezeichne den Vektor $(y_1, \ldots, y_n)$) und nach der Cramerschen Regel ist $A^{adj}A = (\det A)E_n$, also gilt $((\det A)E_n)y = 0$. Es ist also $(\det A)y_j = 0$ für alle j und damit $(\det A)z = 0$ für alle $z \in M$. Da M nach Voraussetzung einen Nichtnullteiler enthält, muss $\det A = 0$ sein.

Die Determinante ist aber ein normierter polynomialer Ausdruck in x vom Grad n, sodass eine Ganzheitsgleichung vorliegt. □

Korollar 11.6. *Seien R und S kommutative Ringe und $R \subseteq S$ eine Ringerweiterung. Dann ist der ganze Abschluss von R in S eine R-Unteralgebra von S.*

Beweis. Die Ganzheitsgleichungen $X - r$, $r \in R$, zeigen, dass jedes Element aus R ganz über R ist. Seien $x_1 \in S$ und $x_2 \in S$ ganz über R. Nach der Charakterisierung der Ganzheit gibt es endliche R-Unteralgebren $T_1, T_2 \subseteq S$ mit $x_1 \in T_1$ und $x_2 \in T_2$. Sei $y_1, \ldots, y_n$ ein R-Erzeugendensystem von T_1 und $z_1, \ldots, z_m$ ein R-Erzeugendensystem von T_2. Wir können annehmen, dass $y_1 = z_1 = 1$ ist. Betrachte den endlich erzeugten R-Modul

$$T \;=\; T_1 \cdot T_2 \;=\; \langle y_i z_j,\, i = 1, \ldots, n,\, j = 1, \ldots, m \rangle,$$

der offensichtlich $x_1 + x_2$ und $x_1 x_2$ (und 1) enthält. Dieser R-Modul T ist auch wieder eine R-Algebra, da für zwei beliebige Elemente gilt

$$\Big(\sum r_{ij} y_i z_j\Big)\Big(\sum s_{kl} y_k z_l\Big) = \sum r_{ij} s_{kl} y_i y_k z_j z_l\,,$$

und für die Produkte gilt $y_i y_k \in T_1$ und $z_j z_l \in T_2$, sodass diese Linearkombination zu T gehört. Dies zeigt, dass die Summe und das Produkt von zwei ganzen Elementen wieder ganz ist. Deshalb ist der ganze Abschluss ein Unterring von S, der R enthält. Also liegt eine R-Unteralgebra vor. □

Definition 11.7. Seien R und S kommutative Ringe und $R \subseteq S$ eine Ringerweiterung. Man nennt R *ganz-abgeschlossen* in S, wenn der ganze Abschluss von R in S gleich R ist.

Ganzheit und Endlichkeit

Eng verwandt mit der Ganzheit $A \subseteq B$ ist die Endlichkeit der Algebra B über A, die einfach bedeutet, dass B ein endlich erzeugter A-Modul ist.

Lemma 11.8. *Es sei S eine endliche R-Algebra und M ein endlich erzeugter S-Modul. Dann ist M auch ein endlich erzeugter R-Modul.*

Beweis. Es sei $s_1, \ldots, s_k$ ein R-Modul-Erzeugendensystem von S und $v_1, \ldots, v_n$ ein S-Modul-Erzeugendensystem von M. Dann bilden die Produkte $s_i v_j$, $1 \le i \le k$, $1 \le j \le n$, ein R-Modul-Erzeugendensystem von M. □

Korollar 11.9. *Es sei S eine endliche R-Algebra und T eine endliche S-Algebra. Dann ist T eine endliche R-Algebra.*

Beweis. Dies folgt direkt aus Lemma 11.8. □

Satz 11.10. *Es sei $\varphi\colon R \to S$ ein ganzer Ringhomomorphismus von endlichem Typ. Dann ist S endlich über R.*

Beweis. Es sei $S = R[x_1, \ldots, x_n]$. Wir betrachten die Kette

$$R \longrightarrow R[x_1] \longrightarrow R[x_1, x_2] \longrightarrow \ldots \longrightarrow R[x_1, \ldots, x_n] = S$$

von ganzen Ringhomomorphismen, die jeweils durch ein Element erzeugt werden. Nach Korollar 11.9 genügt es zu zeigen, dass

$$R \longrightarrow R[x]$$

endlich ist, wenn x eine Ganzheitsgleichung über R erfüllt. Mit der Ganzheitsgleichung lässt sich aber eine Potenz (und damit alle höheren Potenzen) von x als R-Linearkombination der kleineren Potenzen ausdrücken, so dass ein endlich erzeugter R-Modul vorliegt. □

Normale und faktorielle Integritätsbereiche

Definition 11.11. Ein Integritätsbereich heißt *normal*, wenn er ganz-abgeschlossen in seinem Quotientenkörper ist.

Wichtige Beispiele für normale Ringe werden durch faktorielle Ringe geliefert.

Definition 11.12. Ein Integritätsbereich heißt *faktorieller Bereich*, wenn jede Nichteinheit $f \neq 0$ sich als ein Produkt von Primelementen schreiben lässt.

Lemma 11.13. *Sei R ein Integritätsbereich. Dann sind folgende Aussagen äquivalent.*

(1) *R ist faktoriell.*
(2) *Jede Nichteinheit $f \neq 0$ besitzt eine Faktorzerlegung in irreduzible Elemente, und diese Zerlegung ist bis auf Umordnung und Assoziiertheit eindeutig.*
(3) *Jede Nichteinheit $f \neq 0$ besitzt eine Faktorzerlegung in irreduzible Elemente, und jedes irreduzible Element ist ein Primelement.*

Beweis. (1) $\Rightarrow$ (2). Sei $f \neq 0$ eine Nichteinheit. Die Faktorisierung in Primelemente ist insbesondere eine Zerlegung in irreduzible Elemente, so dass also lediglich die Eindeutigkeit zu zeigen ist. Dies geschieht durch Induktion über die minimale Anzahl der Primelemente in einer Faktorzerlegung. Wenn es eine Darstellung $f = p$ mit einem Primelement gibt, und $f = q_1 \cdots q_r$ eine weitere Zerlegung in irreduzible Faktoren ist, so teilt p einen der Faktoren q_i und nach Kürzen durch p erhält man, dass das Produkt der übrigen Faktoren rechts eine Einheit sein muss. Das bedeutet aber, dass es keine weiteren Faktoren geben kann. Sei nun $f = p_1 \cdots p_s$ und diese Aussage sei für Elemente mit kleineren Faktorisierungen in Primelemente bereits bewiesen. Es sei

$$f = p_1 \cdots p_s = q_1 \cdots q_r$$

eine weitere Zerlegung mit irreduziblen Elementen. Dann teilt wieder p_1 einen der Faktoren rechts, sagen wir $p_1 u = q_1$. Dann muss u eine Einheit sein und

wir können durch p_1 kürzen, wobei wir u^{-1} mit q_2 verarbeiten können, was ein assoziiertes Element ergibt. Das gekürzte Element hat eine Faktorzerlegung mit $r-1$ Primelementen, so dass wir die Induktionsvoraussetzung anwenden können. (2) $\Rightarrow$ (3). Wir müssen zeigen, dass ein irreduzibles Element auch prim ist. Sei also q irreduzibel und es teile das Produkt fg, sagen wir

$$qh = fg\,.$$

Für h, f und g gibt es Faktorzerlegungen in irreduzible Elemente, so dass sich insgesamt die Gleichung

$$qh_1 \cdots h_r = f_1 \cdots f_s g_1 \cdots g_t$$

ergibt. Es liegen also zwei Zerlegungen in irreduzible Element vor, die nach Voraussetzung im Wesentlichen übereinstimmen müssen. D.h. insbesondere, dass es auf der rechten Seite einen Faktor gibt, sagen wir f_1, der assoziiert zu q ist. Dann teilt q auch den ursprünglichen Faktor f. (3) $\Rightarrow$ (1). Das ist trivial. □

Der Polynomring über einem Körper ist faktoriell, was wir aber nicht beweisen werden.

Satz 11.14. *Sei R ein faktorieller Integritätsbereich. Dann ist R normal.*

Beweis. Sei $K = Q(R)$ der Quotientenkörper von R und $q \in K$ ein Element, das die Ganzheitsgleichung

$$q^n + r_{n-1}q^{n-1} + r_{n-2}q^{n-2} + \ldots + r_1 q + r_0 = 0$$

mit $r_i \in R$ erfüllt. Wir schreiben $q = a/b$ mit $a, b \in R$, wobei wir annehmen können, dass die Darstellung gekürzt ist, dass also a und $b \in R$ keinen gemeinsamen Primteiler besitzen. Wir haben zu zeigen, dass b eine Einheit in R ist, da dann $q = ab^{-1}$ zu R gehört.

Wir multiplizieren obige Ganzheitsgleichung mit b^n und erhalten in R

$$a^n + (r_{n-1}b)a^{n-1} + (r_{n-2}b^2)a^{n-2} + \ldots + (r_1 b^{n-1})a + (r_0 b^n) = 0\,.$$

Wenn b keine Einheit ist, dann gibt es einen Primteiler p von b. Dieser teilt alle Summanden $(r_{n-i}b^i)a^{n-i}$ für $i \geq 1$ und daher auch den ersten, also a^n. Das bedeutet aber, dass a selbst ein Vielfaches von p ist im Widerspruch zur vorausgesetzten Teilerfremdheit. □

Definition 11.15. Sei R ein Integritätsbereich und $Q(R)$ sein Quotientenkörper. Dann nennt man den ganzen Abschluss von R in $Q(R)$ die *Normalisierung* von R.

11. Arbeitsblatt

Aufwärmaufgaben

Aufgabe 11.1. Sei $R \subseteq S$ eine ganze Erweiterung von Integritätsbereichen und sei $F \subseteq R$ ein multiplikatives System. Zeige, dass dann auch die zugehörige Erweiterung $R_F \subseteq S_F$ ganz ist.

Aufgabe 11.2.*

Seien R und S Integritätsbereiche und sei $R \subseteq S$ eine ganze Ringerweiterung. Es sei $f \in R$ ein Element, das in S eine Einheit ist. Zeige, dass f dann schon in R eine Einheit ist.

Aufgabe 11.3. Sei R ein kommutativer Ring und A eine R-Algebra. Zeige, dass wenn R ein Körper ist, die Begriffe algebraisch und ganz für ein Element $x \in A$ übereinstimmen. Zeige ferner, dass für einen Integritätsbereich, der kein Körper ist, diese beiden Begriffe auseinanderfallen.

Aufgabe 11.4. Man gebe ein Beispiel einer ganzen Ringerweiterung $R \subseteq S$, wo es einen Nichtnullteiler $f \in R$ gibt, der ein Nullteiler in S wird.

Aufgabe 11.5. Sei K ein Körper und sei $R_i \subseteq K$, $i \in I$, eine Familie von normalen Unterringen. Zeige, dass auch der Durchschnitt $\bigcap_{i \in I} R_i$ normal ist.

Aufgabe 11.6. Sei R ein Integritätsbereich. Zeige, dass R genau dann normal ist, wenn er mit seiner Normalisierung übereinstimmt.

Aufgabe 11.7. Sei R ein Integritätsbereich. Sei angenommen, dass die Normalisierung von R gleich dem Quotientenkörper $Q(R)$ ist. Zeige, dass dann R selbst schon ein Körper ist.

Aufgabe 11.8.*

Sei R ein normaler Integritätsbereich und $f \in R$, $f \neq 0$. Zeige, dass die Nenneraufnahme R_f ebenfalls normal ist.

Aufgabe 11.9. Sei R ein normaler Integritätsbereich und sei $S \subseteq R$ ein multiplikatives System. Zeige, dass dann auch die Nenneraufnahme R_S normal ist.

Aufgabe 11.10. Sei R ein faktorieller Bereich. Zeige, dass jedes von null verschiedene Primideal ein Primelement enthält.

Aufgaben zum Abgeben

Aufgabe 11.11. (3 Punkte)

Seien R, S, T kommutative Ringe und seien $\varphi : R \to S$ und $\psi : S \to T$ Ringhomomorphismen derart, dass S ganz über R und T ganz über S ist. Zeige, dass dann auch T ganz über R ist.

Aufgabe 11.12. (3 Punkte)

Sei K ein algebraisch abgeschlossener Körper und $F \in K[X,Y]$ ein nichtkonstantes Polynom. Zeige, dass der Restklassenring

$$K[X,Y]/(F)$$

eine endliche $K[T]$-Algebra ist.

Aufgabe 11.13. (3 Punkte)

Sei K ein Körper und A eine endliche K-Algebra. Zeige: Dann ist A artinsch.

Aufgabe 11.14. (3 Punkte)

Sei R ein normaler Integritätsbereich und $R \subseteq S$ eine ganze Ringerweiterung. Sei $f \in R$. Zeige, dass für das von f erzeugte Hauptideal gilt:

$$R \cap (f)S = (f)R\,.$$

Aufgabe 11.15. (6 Punkte)

Sei R ein normaler Integritätsbereich. Zeige, dass dann auch der Polynomring $R[X]$ normal ist.

Aufgabe 11.16. (5 Punkte)

Sei R ein normaler Integritätsbereich und $a \in R$. Es sei vorausgesetzt, dass a keine Quadratwurzel in R besitzt. Zeige, dass das Polynom $X^2 - a$ prim in $R[X]$ ist. Tipp: Verwende den Quotientenkörper $Q(R)$. Warnung: Prim muss hier nicht zu irreduzibel äquivalent sein.

Aufgabe 11.17. (4 Punkte)

Sei R ein Integritätsbereich. Zeige, dass die folgenden Eigenschaften äquivalent sind.

(1) R ist normal
(2) Für jedes Primideal $\mathfrak{p}$ ist die Lokalisierung $R_{\mathfrak{p}}$ normal.
(3) Für jedes maximale Ideal $\mathfrak{m}$ ist die Lokalisierung $R_{\mathfrak{m}}$ normal.

(Man sagt daher, dass normal eine *lokale Eigenschaft* ist.)

Aufgabe 11.18. (4 Punkte)

Seien $M \subseteq N$ endlich erzeugte kommutative Monoide. Zeige, dass für einen Körper K der Ringhomomorphismus $K[M] \subseteq K[N]$ genau dann endlich ist, wenn es zu jedem $n \in N$ ein $k \in \mathbb{N}_+$ mit $kn \in M$ gibt.

12. Vorlesung - Endlichkeitssätze

Wir kommen nun zu wichtigen Folgerungen der in den letzten beiden Vorlesungen entwickelten Begriffe für die Invariantentheorie.

Ganzheit und Invariantenringe

Lemma 12.1. *Es sei R ein kommutativer Ring, auf dem eine endliche Gruppe G durch Ringautomorphismen operiere. Dann ist $R^G \subseteq R$ eine ganze Erweiterung.*

Beweis. Zu $f \in R$ betrachten wir das Produkt

$$P = \prod_{\sigma \in G} (X - f\sigma) \in R[X]\,.$$

Die Koeffizienten dieses Polynoms gehören zum Invariantenring R^G. Ferner ist P normiert und es ist $P(f) = 0$ (da ja $X - fe_G = X - f$ ein Linearfaktor ist). Somit liefert P eine Ganzheitsgleichung für f über R^G und daher ist $R^G \subseteq R$ ganz. □

Satz 12.2. *Es sei R ein normaler Integritätsbereich und G eine Gruppe, die auf R als Gruppe von Ringautomorphismen operiere. Dann ist auch der Invariantenring normal.*

Beweis. Es sei $q \in Q\left(R^G\right) \subseteq Q(R)$ und q erfülle eine Ganzheitsgleichung über R^G. Wegen $R^G \subseteq R$ ist q auch ganz über R und wegen der Normalität von R muss $q \in R$ gelten. Wegen

$$R \cap Q\left(R^G\right) \;=\; R^G$$

ist somit $q \in R^G$, also ist R^G normal. □

Es ist eine wichtige Frage, welche weiteren Eigenschaften eines Ringes sich - unter welchen Bedingungen - auf einen Invariantenring übertragen. Für die endliche Erzeugtheit werden wir das im Folgenden behandeln, für die Faktorialität weiter unten. Die Eigenschaft, dass der Invariantenring bei einer linearen Operation ein Polynomring (also „regulär“) ist, werden wir später ausführlich behandeln.

Der Satz von Noether

Der folgende Satz heißt *Satz von Noether*.

Satz 12.3. *Es sei K ein Körper, R eine endlich erzeugte kommutative K-Algebra, auf der eine endliche Gruppe G durch K-Algebraautomorphismen operiere. Dann ist der Invariantenring R^G eine endlich erzeugte K-Algebra.*

Beweis. Sei

$$R = K[f_1, \ldots, f_n].$$

Nach Lemma 12.1 ist $R^G \subseteq R$ eine ganze Erweiterung. Zu jedem f_i gibt es daher eine Ganzheitsgleichung

$$f_i^{n_i} + a_{i,n_i-1} f_i^{n_i-1} + \ldots + a_{i,1} f_i + a_{i,0} = 0$$

mit $a_{i,j} \in R^G$. Wir betrachten die von den Koeffizienten $a_{i,j}$ erzeugte K-Unteralgebra von R^G, also

$$S := K[a_{i,j},\, 1 \leq i \leq n,\, 0 \leq j < n_i] \subseteq R^G.$$

Dabei ist S endlich erzeugt, und sämtliche Ganzheitsgleichungen sind über S formulierbar, d.h. nach Korollar 11.6, dass R auch über S ganz ist. Da S über K endlich erzeugt ist, ist R insbesondere über S endlich erzeugt, so dass $S \subseteq R$ nach Satz 11.10 sogar endlich ist. Da S noethersch ist, muss nach Satz 10.13 auch die S-Unteralgebra $R^G \subseteq R$ ein endlicher S-Modul sein. Damit ist insgesamt R^G eine endlich erzeugte K-Algebra. □

Aus Lemma 12.1 und Satz 12.3 folgt in Zusammenhang mit Satz 11.10, dass $R^G \subseteq R$ eine endliche Abbildung ist.

Bemerkung 12.4. Das *14. Hilbertsche Problem* ist die Frage, ob für jede Gruppenoperation auf einer endlich erzeugten K-Algebra auch der Invariantenring R^G endlich erzeugt ist. Es wurde von Hilbert 1900 auf dem internationalen Mathematikerkongress in Paris als eines seiner 23 mathematischen Probleme vorgestellt und in den späten Fünfzigern durch ein Gegenbeispiel von Masayoshi Nagata negativ beantwortet.

Der Satz von Hilbert

Wir geben einen weiteren Beweis für den Endlichkeitssatz unter der Voraussetzung, dass der Invariantenring ein direkter Summand ist. Die dabei operierende Gruppe muss nicht endlich sein. Die Voraussetzung, dass es einen Reynolds-Operator gibt, ist für endliche Gruppen erfüllt, wenn ihre Ordnung kein Vielfaches der Charakteristik ist. Sie ist ferner für die sogenannten linear-reduktiven Gruppen in Charakteristik 0 erfüllt, also beispielsweise für die allgemeine lineare Gruppe, was wir später zeigen werden.

Definition 12.5. Es sei K ein Körper. Eine $\mathbb{Z}$-graduierte kommutative K-Algebra R heißt *positiv-graduiert*, wenn $R_d = 0$ für $d < 0$ und $R_0 = K$ ist.

Insbesondere kann man den Polynomring positiv graduieren, wenn man jeder Variablen einen positiven Grad $\operatorname{grad}(X_i) = d_i \in \mathbb{N}_{>0}$ zuweist.

Lemma 12.6. *Es sei G eine Gruppe, die auf dem positiv graduierten Polynomring $K[X_1, \ldots, X_n]$ als Gruppe von homogenen Ringautomorphismen operiere. Es sei I_G das von allen homogenen Invarianten positiven Grades erzeugte Ideal in $K[X_1, \ldots, X_n]$ und es sei $g_1, \ldots, g_m$ ein homogenes Idealerzeugendensystem dieses Ideals. Es sei vorausgesetzt, dass der Invariantenring ein homogener direkter Summand des Polynomringes ist. Dann bilden die $g_1, \ldots, g_m$ ein Algebraerzeugendensystem des Invariantenringes, d.h. es ist*

$$K[X_1, \ldots, X_n]^G = K[g_1, \ldots, g_m].$$

Beweis. Aufgrund der Homogenität der Operation ist der Invariantenring selbst positiv graduiert. Wir beweisen die Inklusion

$$K[X_1, \ldots, X_n]^G \subseteq K[g_1, \ldots, g_m]$$

durch Induktion über den Grad. Wir betrachten also ein homogenes Element $f \in K[X_1, \ldots, X_n]^G$ von positivem Grad. Wegen $f \in I_G$ kann man

$$f = \sum_{j=1}^{m} h_j g_j$$

mit homogenen Elementen h_j von einem Grad $< \operatorname{grad}(f)$ schreiben. Der Reynolds-Operator

$$\rho\colon\ K[X_1, \ldots, X_n] \longrightarrow K[X_1, \ldots, X_n]^G,$$

angewendet auf diese Gleichung, liefert

$$f = \rho(f) = \rho\left(\sum_{j=1}^{m} h_j g_j\right) = \sum_{j=1}^{m} \rho(h_j)\, g_j.$$

Dabei ist der Grad der $\rho(h_j)$ gleich dem Grad der h_j und somit kleiner als der Grad von f und sie gehören zum Invariantenring, so dass die $\rho(h_j)$ nach Induktionsvoraussetzung in der von den g_j erzeugten Algebra liegen. □

Korollar 12.7. *Es sei G eine Gruppe, die auf dem positiv graduierten Polynomring $K[X_1, \ldots, X_n]$ als Gruppe von homogenen K-Algebraautomorphismen operiere. Es sei vorausgesetzt, dass der Invariantenring ein homogener direkter Summand des Polynomringes ist. Dann ist der Invariantenring eine endlich erzeugte K-Algebra.*

Beweis. Es sei I_G das von allen Invarianten positiven Grades erzeugte Ideal in $K[X_1, \ldots, X_n]$. Aufgrund des Hilbertschen Basissatzes besitzt I_G ein endliches Idealerzeugendensystem. Daher folgt die Aussage aus Lemma 12.6. □

Faktorialität der Invariantenringe

Während Invariantenringe unter schwachen Voraussetzungen normal sind, ist die Faktorialität eher eine seltene Eigenschaft. In Beispiel 7.13 haben wir eine lineare Operation einer zyklischen Gruppe $\mathbb{Z}/(n)$ auf $K[U, V]$ kennengelernt, deren Invariantenring gleich $K[X, Y, Z]/(XY - Z^n)$ ist. Die Gleichung $XY = Z^n$ zeigt, dass eine zwei wesentlich verschiedene Zerlegungen in irreduzible Elemente vorliegt. Dieser Invariantenring ist also nicht fakoriell.

Satz 12.8. *Es sei R ein faktorieller Bereich und es sei G eine endliche Gruppe, die auf R als Gruppe von Ringautomorphismen operiere. Die Charaktergruppe zu G mit Werten in der Einheitengruppe $R^\times$ sei trivial, d.h. es ist*

$$\operatorname{Hom}\left(G, R^\times\right) = 0.$$

Dann ist auch der Invariantenring faktoriell.

Beweis. Wir zeigen, dass $F \in R^G$, $F \neq 0$, eine im Wesentlichen eindeutige Zerlegung in irreduzible Faktoren besitzt. Sei

$$F = F_1^{r_1} \cdots F_n^{r_n}$$

die Zerlegung in R in irreduzible Faktoren, wobei die F_i paarweise nicht (in R) assoziiert seien. Für jedes $\sigma \in G$ ist dann auch

$$F = F\sigma = (F_1\sigma)^{r_1} \cdots (F_n\sigma)^{r_n}.$$

Wegen der Faktorialität von R muss diese Zerlegung mit der ursprünglichen Faktorzerlegung übereinstimmen, d.h. zu jedem i gibt es ein j und eine Einheit $a_{ij} \in R^\times$ mit

$$F_i\sigma = a_{ij}F_j.$$

Es sei

$$\{1, \ldots, n\} = \biguplus_{j \in J} I_j$$

die disjunkte Zerlegung der Indexmenge, bei der zwei Indizes i, j in der gleichen Teilmenge landen, wenn es ein $\sigma \in G$ gibt derart, dass $F_i\sigma$ und F_j assoziiert sind. Wir setzen

$$H_j := \prod_{i \in I_j} F_i.$$

Insbesondere ist dann

$$F = \prod_{j \in J} H_j^{r_j}.$$

Es ist

$$H_j\sigma = \left(\prod_{i \in I_j} F_i \right) \sigma = \prod_{i \in I_j} (F_i\sigma) = a_j(\sigma) \prod_{i \in I_j} F_i = a_j(\sigma) H_j$$

mit einer (von σ abhängigen) Einheit

$$a_j(\sigma) = \frac{H_j\sigma}{H_j}.$$

An dieser letzten Darstellung sieht man, dass die Zuordnung $G \to R^\times$, $\sigma \mapsto a_j(\sigma)$, ein Charakter ist. Nach Voraussetzung ist dieser also trivial, und damit sind die H_j invariant. Somit ist

$$F = \prod_{j \in J} H_j$$

eine Faktorzerlegung in R^G. Die H_j sind dabei irreduzibel in R^G, da eine Faktorzerlegung $H = AB$ sofort zu einer Zerlegung von $H_j = \prod_{i \in I_j} F_i$ in Teilprodukte führt, die aber wegend er Wahl der I_j nicht invariant sein können. Wenn $F = \prod_\ell A_\ell$ eine beliebige Zerlegung von F in irreduzible Faktoren $A_\ell \in R^G$ ist, so sind die A_ℓ, aufgefasst in R, Produkte gewisser F_i, und wegen der Wahl der I_j wird A_ℓ sogar von einem H_j (in R und in R^G) geteilt. Es liegt also eine eindeutige Zerlegung in irreduzible Faktoren vor und damit ist nach Lemma 11.13 (2) faktoriell. □

Korollar 12.9. *Es sei K ein Körper und $R = K[X_1, \ldots, X_n]$. Es sei G eine endliche Gruppe, die auf R als Gruppe von K-Algebraautomorphismen operiere. Die Charaktergruppe $G^\vee$ sei trivial. Dann ist auch der Invariantenring faktoriell.*

Beweis. Dies folgt aus Satz 12.8. □

Das Beispiel der symmetrischen Gruppe zusammen mit dem nichttrivialen Signumscharakter, wo der Invariantenring ein Polynomring ist, zeigt, dass die Bedingung des vorstehenden Satzes nicht notwendig für die Faktorialität des Invariantenringes ist.

Die Krulldimension

Definition 12.10. Sei R ein kommutativer Ring. Eine Kette aus Primidealen

$$\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \ldots \subset \mathfrak{p}_n$$

nennt man *Primidealkette der Länge n* (es wird also die Anzahl der Inklusionen gezählt, nicht die Anzahl der beteiligten Primideale). Die *Dimension* (oder *Krulldimension*) von R ist das Supremum über alle Längen von Primidealketten. Sie wird mit $\dim(R)$ bezeichnet.

Wir werden hier die Dimensionstheorie nicht systematisch entwickeln. Ohne Beweis teilen wir das folgende Ergebnis mit.

Satz 12.11. *Es sei R ein noetherscher Ring der Dimension d. Dann besitzt der Polynomring $R[X]$ die Dimension $d+1$.*

Insbesondere ist die Dimension des Polynomringes $K[X_1, \ldots, X_n]$ über einem Körper K gleich n. Wir werden bald, ausgehend von der Ganzheit über dem Invariantenring, sehen, dass der Invariantenring dimensionsgleich zum Ausgangsring ist.

12. Arbeitsblatt

Aufwärmaufgaben

Aufgabe 12.1. Es sei D eine endliche kommutative Gruppe und R ein D-graduierter Ring. Zeige, dass R ganz über der neutralen Stufe R_0 ist.

Aufgabe 12.2. Es sei D eine kommutative Gruppe und R ein D-graduierter normaler Integritätsbereich. Zeige, dass dann auch die neutrale Stufe R_0 normal ist.

Aufgabe 12.3. Wir betrachten die natürliche Operation der symmetrischen Gruppe S_n auf dem Polynomring $K[X_1, \ldots, X_n]$ über einem Körper K. Bestimme eine Ganzheitsgleichung für die Variablen X_i über dem Invariantenring.

Aufgabe 12.4. Begründe, dass $K[x,y] \subseteq K[x,y,z]/(xy - z^n)$ endlich ist. Wie sieht es über $K[x,z]$ bzw. $K[y,z]$ aus?

Aufgabe 12.5. Begründe, dass $K[y,z] \subseteq K[x,y,z]/(x^2+yz^2+z^{m+1})$ endlich ist. Wie sieht es über $K[x,y]$ bzw. $K[x,z]$ aus?

Aufgabe 12.6. Wir betrachten die natürliche Operation der alternierenden Gruppe A_n auf dem $K[X_1, \ldots, X_n]$. Für welche $n \in \mathbb{N}$ ist der Invariantenring $K[X_1, \ldots, X_n]^{A_n}$ faktoriell?

Aufgabe 12.7. Sei K ein Körper und $s \in \mathbb{N}_+$. Bestimme den Typ des s-ten Veronese-Ringes $K[U, V]^{(s)}$. Für welche s handelt es sich um einen Gorenstein-Ring?

Es sei R ein kommutativer Ring, auf dem eine Gruppe G als Gruppe von Ringautomorphismen operiere, und es sei V ein R-Modul. Eine Operation von G auf V als Gruppe von R-Modulautomorphismen heißt *verträglich* (bezüglich der Operation von G auf R), wenn

$$(f\sigma) \cdot (v\sigma) \;=\; (f \cdot v)\sigma$$

für alle $\sigma \in G$, $f \in R$ und $v \in V$ gilt.

Aufgabe 12.8. Es sei R ein kommutativer Ring, auf dem eine Gruppe G als Gruppe von Ringautomorphismen operiere. Es sei V ein R-Modul, auf dem G als Gruppe von R-Modulautomorphismen operiere, wobei die beiden Operationen verträglich seien. Zeige, dass der Fixmodul V^G ein R^G-Modul.

Aufgabe 12.9. Sei R ein Hauptidealbereich, der kein Körper sei. Zeige, dass die Krulldimension von R gleich eins ist.

Aufgabe 12.10. Es sei $\varphi\colon R \to S$ ein surjektiver Ringhomomorphismus zwischen den Integritätsbereichen R und S. Die Krulldimension dieser Ringe sei endlich und gleich. Zeige, dass dann φ ein Isomorphismus ist.

Aufgabe 12.11. Sei R ein kommutativer Ring von endlicher Krulldimension d. Zeige, dass die Krulldimension des Polynomrings $R[X]$ mindestens $d + 1$ ist.

Aufgaben zum Abgeben

Aufgabe 12.12. (3 Punkte)

Es sei K ein Körper und R eine kommutative K-Algebra, auf dem eine endliche Gruppe G als Gruppe von K-Algebraautomorphismen operiere. Es sei

$$\chi\colon G \longrightarrow K^\times$$

ein Charakter. Zeige, dass zu jedem $f \in R$ die Summe

$$\sum_{\sigma \in G} \frac{f\sigma}{\chi(\sigma)}$$

zu R_χ^G gehört.

Aufgabe 12.13. (4 Punkte)

Es sei K ein Körper und R eine integre K-Algebra, auf dem eine endliche Gruppe G als Gruppe von K-Algebraautomorphismen operiere. Es sei

$$\chi\colon\ G \longrightarrow K^\times$$

ein Charakter und R_χ^G der zugehörige R^G-Modul der Semiinvarianten. Es sei $R_\chi^G \neq 0$ vorausgesetzt. Zeige, dass es einen R^G-Modulhomomorphismus $\varphi\colon\ R^G \to R_\chi^G$ derart gibt, dass φ nach Nenneraufnahme an einem Element $f \in R^G$, $f \neq 0$, ein Isomorphismus wird.

Aufgabe 12.14. (4 Punkte)

Es sei K ein Körper und $K[U,V]$ sei mit der $\mathbb{Z}/(n)$-Graduierung versehen, bei der U den Grad 1 und V den Grad -1 bekommt. Zeige, dass die Stufen R_d, $d \neq 0$, (als R_0-Moduln) nicht isomorph zu R_0 sind.

Aufgabe 12.15. (4 Punkte)

Sei K ein algebraisch abgeschlossener Körper und sei $R = K[X,Y]$ der Polynomring in zwei Variablen. Zeige, dass R die Krulldimension zwei besitzt.

13. Vorlesung - Das Spektrum I

Das Spektrum eines kommutativen Ringes

Bei einer linearen Operation einer Gruppe G auf einem K-Vektorraum V haben wir einerseits die Operation auf dem geometrischen Objekt, nämlich dem Vektorraum, und andererseits die Operation auf dem zugehörigen Polynomring als Gruppe von Ringautomorphismen. Es ist wünschenswert, zu einer solchen algebraischen Operation auf einem beliebigen kommutativen Ring auch eine geometrische Interpretation zu besitzen. Dieses (und vieles andere) leistet das *Spektrum* eines kommutativen Ringes.

Alexander Grothendieck (1928-)

Definition 13.1. Zu einem kommutativen Ring R nennt man die Menge der Primideale von R das *Spektrum* von R, geschrieben

$$\text{Spek}\,(R)\ .$$

Man spricht auch von einem *affinen Schema*.

Definition 13.2. Auf dem Spektrum eines kommutativen Ringes R ist die *Zariski-Topologie* dadurch gegeben, dass zu einer beliebigen Teilmenge $T \subseteq R$ die Mengen

$$D(T) := \{\mathfrak{p} \in \text{Spec } R | \, \mathfrak{p} \not\subseteq T\}$$

als offen erklärt werden.

Für einelementige Teilmengen $T = \{f\}$ schreiben wir $D(f)$ statt $D(\{f\})$.

Lemma 13.3. *Die Zariski-Topologie auf dem Spektrum* $\text{Spek}\,(R)$ *eines kommutativen Ringes R ist in der Tat eine Topologie.*

Beweis. Es ist $D(0) = \emptyset$ und $D(1) = \text{Spek}\,(R)$, da jedes Primideal die 0 und kein Primideal die 1 enthält.

Zu einer beliebigen Familie T_i, $i \in I$, aus Teilmengen $T_i \subseteq R$ ist

$$\bigcup_{i\in I} D(T_i) \ = \ D\left(\bigcup_{i\in I} T_i\right).$$

Dabei ist die Inklusion $\subseteq$ klar, da $T_i \subseteq \bigcup_{i\in I} T_i$ gilt und da aus $S \subseteq T$ stets $D(S) \subseteq D(T)$ folgt. Für die andere Inklusion sei $\mathfrak{p} \in D\left(\bigcup_{i\in I} T_i\right)$. D.h. es gibt ein $f \in \bigcup_{i\in I} T_i$ mit $f \notin \mathfrak{p}$. Somit gibt es ein $i \in I$ mit $f \in T_i$ und daher $\mathfrak{p} \in D(T_i)$ für dieses i.

Zu einer endlichen Familie $T_1, \ldots, T_n$ aus Teilmengen $T_i \subseteq R$ ist

$$\bigcap_{i=1}^{n} D(T_i) \;=\; D(T_1 \cdots T_n).$$

Dabei bezeichnet $T_1 \cdots T_n$ die Menge aller Produkte $f_1 \cdots f_n$ mit $f_i \in T_i$. Hierbei ist die Inklusion $\supseteq$ klar. Für die umgekehrte Inklusion sei $\mathfrak{p} \in D(T_i)$ für alle $i = 1, \ldots, n$ vorausgesetzt. Das bedeutet, dass es $f_i \in T_i$ mit $f_i \notin \mathfrak{p}$ gibt. Aufgrund der Primidealeigenschaft ist dann $f_1 \cdots f_n \notin \mathfrak{p}$, also $\mathfrak{p} \in D(T_1 \cdots T_n)$. □

Wir betrachten das Spektrum stets als topologischen Raum. Die Primideale sind die Punkte dieses Raumes. Wir schreiben häufig $X = \operatorname{Spek}(R)$ und $x \in X$, um die geometrische Sichtweise zu betonen. Für das Primideal, das durch x repräsentiert wird, schreibt man dann wiederum $\mathfrak{p}_x$.

Die Komplemente der offenen Mengen, also die abgeschlossenen Mengen in der Zariski-Topologie, werden mit

$$V(T) = \{\mathfrak{p} \in \operatorname{Spek}(R) \mid T \subseteq \mathfrak{p}\}$$

bezeichnet.

Proposition 13.4. *Für das Spektrum $X = \operatorname{Spek}(R)$ eines kommutativen Ringes R gelten folgende Eigenschaften.*

(1) *Es ist $D(T) = D(\mathfrak{a})$, wobei $\mathfrak{a}$ das durch T erzeugte Ideal (Radikal) in R sei. Man kann sich also bei der Beschreibung der offenen Teilmengen auf die Radikale von R beschränken.*
(2) *Für eine Familie $\mathfrak{a}_i$, $i \in I$, von Idealen in R ist*

$$\bigcup_{i \in I} D(\mathfrak{a}_i) \;=\; D\left(\sum_{i \in I} \mathfrak{a}_i\right).$$

(3) *Für eine endliche Familie $\mathfrak{a}_i$, $i = 1, \ldots, n$, von Idealen in R ist*

$$\bigcap_{i=1}^{n} D(\mathfrak{a}_i) \;=\; D\left(\bigcap_{i=1}^{n} \mathfrak{a}_i\right) \;=\; D(\mathfrak{a}_1 \cdots \mathfrak{a}_n).$$

(4) *Es ist $D(\mathfrak{a}) = X$ genau dann, wenn $\mathfrak{a}$ das Einheitsideal ist.*
(5) *Es ist $D(\mathfrak{a}) \subseteq D(\mathfrak{b})$ genau dann, wenn $\mathfrak{a} \subseteq \operatorname{rad}(\mathfrak{b})$ gilt.*
(6) *Das Spektrum ist genau dann leer, wenn R der Nullring ist.*
(7) *Es ist $D(\mathfrak{a}) = \emptyset$ genau dann, wenn $\mathfrak{a}$ nur nilpotente Element enthält.*
(8) *Die offenen Mengen $D(f)$, $f \in R$, bilden eine Basis der Topologie.*
(9) *Eine Familie von offenen Mengen $D(\mathfrak{a}_i)$, $i \in I$, ist genau dann eine Überdeckung von X, wenn die Ideale $\mathfrak{a}_i$ zusammen das Einheitsideal erzeugen.*

Beweis. (1). Die Inklusion $\subseteq$ ist klar. Die andere Inklusion beweisen wir durch Kontraposition und nehmen $\mathfrak{p} \notin D(T)$ an. Dann ist $T \subseteq \mathfrak{p}$ und somit gilt

$$\mathfrak{a} \subseteq \operatorname{rad}(\mathfrak{a}) \subseteq \mathfrak{p},$$

da ein Primideal ein Radikalideal ist. Daher ist auch $\mathfrak{p} \notin D(\operatorname{rad}(\mathfrak{a}))$. (2) und (3) sind klar nach (1) und dem Beweis zu Lemma 13.3. (4). Wenn $\mathfrak{a}$ nicht das Einheitsideal ist, so gibt es nach Aufgabe 13.6 ein maximales Ideal $\mathfrak{a} \subseteq \mathfrak{m}$, also $\mathfrak{m} \notin D(\mathfrak{a})$. (5). Die Implikation von rechts nach links ist klar. Für die Umkehrung sei $\mathfrak{a} \not\subseteq \operatorname{rad}(\mathfrak{b})$ vorausgesetzt. Dann gibt es ein $f \in \mathfrak{a}$ mit $f^n \notin \mathfrak{b}$ für alle $n \in \mathbb{N}$. Dann gibt es auch ein Primideal $\mathfrak{p} \supseteq \mathfrak{b}$ mit $f \notin \mathfrak{p}$. Also ist $\mathfrak{p} \in D(\mathfrak{a})$ und $\mathfrak{p} \notin D(\mathfrak{b})$. (6). Der Nullring besitzt kein Primideal. Ein vom Nullring verschiedener kommutativer Ring besitzt nach Aufgabe 13.6 maximale Ideale. (7). Jedes Primideal enthält sämtliche nilpotenten Elemente, also ist $V(\mathfrak{a}) = X$ für ein solches Ideal. Wenn dagegen $\mathfrak{a}$ ein nicht nilpotentes Element f enthält, so gibt es nach Aufgabe 13.7 auch ein Primideal $\mathfrak{p}$ mit $f \notin \mathfrak{p}$, also ist $\mathfrak{p} \in D(f) \subseteq D(\mathfrak{a})$. (8). Dies folgt direkt aus $D(\mathfrak{a}) = \bigcup_{f \in \mathfrak{a}} D(f)$. (9) folgt aus und (2) und (4). □

Proposition 13.5. *Für das Spektrum $X = \operatorname{Spek}(R)$ eines kommutativen Ringes R gelten folgende Eigenschaften.*

1. *Der Abschluss einer Teilmenge $T \subseteq X$ ist $V\left(\bigcap_{x \in T} \mathfrak{p}_x\right)$.*
2. *Der Abschluss eines Punktes $x \in X$ ist $V(\mathfrak{p}_x)$.*
3. *Ein Punkt $x \in \operatorname{Spek}(R)$ ist genau dann abgeschlossen, wenn $\mathfrak{p}_x$ ein maximales Ideal ist.*

Beweis. (1). Für $y \in T$ ist $y \in V(\mathfrak{p}_y) \subseteq V\left(\bigcap_{x \in T} \mathfrak{p}_x\right)$, so dass die angegebene Menge eine abgeschlossene Menge ist, die T umfasst. Sei $\mathfrak{q}$ ein Primideal mit $\mathfrak{q} \in V\left(\bigcap_{x \in T} \mathfrak{p}_x\right)$, also $\bigcap_{x \in T} \mathfrak{p}_x \subseteq \mathfrak{q}$. Um zu zeigen, dass $\mathfrak{q}$ auch zum Abschluss von T gehört, muss man zeigen, dass T jede offene Umgebung von $\mathfrak{q}$ schneidet. Sei also $\mathfrak{q} \in D(f)$, d.h. $f \notin \mathfrak{q}$. Dann ist auch $f \notin \bigcap_{x \in T} \mathfrak{p}_x$ und somit gibt es ein $x \in T$ mit $f \notin \mathfrak{p}_x$. Also ist $\mathfrak{p}_x \in D(f)$ und somit $T \cap D(f) \neq \emptyset$. (2) ist ein Spezialfall von (1). (3) folgt aus (2). □

Vor der nächsten Aussage erinnern wir an die (Quasi)-Kompaktheit von topologischen Räumen: Ein topologischer Raum X heißt *kompakt* (oder *überdeckungskompakt*), wenn es zu jeder offenen Überdeckung

$$X = \bigcup_{i \in I} U_i \quad \text{mit } U_i \text{ offen und einer beliebigen Indexmenge}$$

eine endliche Teilmenge $J \subseteq I$ gibt derart, dass

$$X = \bigcup_{i \in J} U_i$$

ist. Häufig spricht man von kompakt nur, wenn der Raum neben dieser Überdeckungseigenschaft auch hausdorffsch ist, und nennt dann die Überdeckungseigenschaft die Quasikompaktheit.

Korollar 13.6. *Das Spektrum $X = \operatorname{Spek}(R)$ eines kommutativen Ringes R ist quasikompakt.*

Beweis. Nach Proposition 13.4 (9) ist $X = \bigcup_{i\in I} D(\mathfrak{a}_i)$ genau dann, wenn die Ideale $\mathfrak{a}_i$, $i \in I$, zusammen das Einheitsideal erzeugen. Das von der Familie erzeugte Ideal besteht aus allen endlichen Summen $f_1 + \ldots + f_n$ mit $f_j \in \mathfrak{a}_{i_j}$. Wenn also das Einheitsideal erzeugt wird, so bedeutet dies, dass es eine endliche Auswahl $\{i_1, \ldots, i_n\} \subseteq I$ und Elemente $f_j \in \mathfrak{a}_{i_j}$ gibt mit $\sum_{j=1}^n f_j = 1$. Dann ist aber

$$X \;=\; D(1) \;=\; \bigcup_{j=1}^{n} D(f_j) \;=\; \bigcup_{j=1}^{n} D(\mathfrak{a}_{i_j})$$

und somit ist eine endliche überdeckende Teilfamilie gefunden. □

Das Spektrum ist nur in Ausnahmesituationen ein Hausdorffraum, d.h. im Allgemeinen kann man zwei Punkte des Spektrums nicht durch offene Umgebungen trennen.

Beispiel 13.7. Ein Körper hat bekanntlich nur zwei Ideale, nämlich das Einheitsideal K, das kein Primideal ist, und das Nullideal 0, das ein Primideal ist. Das Spektrum eines Körpers besteht also aus einem einzigen Punkt.

Beispiel 13.8. Die Primideale in $\mathbb{Z}$ sind einerseits die maximalen Ideale (p), wobei p eine Primzahl ist, und andererseits das Nullideal 0. Die maximalen Ideale bilden die abgeschlossenen Punkte von $\operatorname{Spek}(\mathbb{Z})$. Das Nullideal ist darin ein weiterer nicht abgeschlossener Punkt. Die einzige abgeschlossene Menge, in der dieser Punkt enthalten ist, ist die ganze Menge. Die abgeschlossenen Mengen in $\operatorname{Spek}(\mathbb{Z})$ sind neben der Gesamtmenge die endlichen Teilmengen aus maximalen Idealen.

Man visualisiert $\operatorname{Spek}(\mathbb{Z})$ als eine (gedachte Gerade), auf der die Primzahlen diskret liegen, während der Nullpunkt ein fetter Punkt ist, der die gesamte Gerade representiert.

Beispiel 13.9. Für den Polynomring $R = K[X_1, \ldots, X_n]$ über einem Körper K vermitteln die sogenannten Punktideale eine gute geometrische Vorstellung von $\operatorname{Spek}(R)$. Ein Punktideal hat die Form

$$(X_1 - a_1, X_2 - a_2, \ldots, X_n - a_n)$$

zu einem festen Tupel $a = (a_1, a_2, \ldots, a_n) \in K^n$. Ein Punktideal ist der Kern des durch $X_i \mapsto a_i$ festgelegten K-Algebrahomomorphismus

$$\varphi_a \colon\; R \longrightarrow K$$

und daher ein maximales Ideal. Diese Zuordnung definiert insgesamt eine injektive Abbildung

$$K^n \longrightarrow \operatorname{Spek}(R)\,.$$

Wenn K algebraisch abgeschlossen ist, werden dadurch sogar alle maximale Ideale von R erfasst. Daher stellt man sich das Spektrum des Polynomrings in n Variablen als den affinen Raum vor, der allerdings auch noch weitere nichtabgeschlossene Punkte enthält. Zu einem Polynom $f \in K[X_1, \ldots, X_n]$ besitzt $V(f) \cap K^n$ eine anschauliche Interpretation: Es ist $a \in V(f) \cap K^n$ genau dann, wenn $f(a_1, \ldots, a_n) = 0$ ist.

Auch wenn ein beliebiger endlichdimensionaler K-Vektorraum V mit dem zugehörigen Polynomring $K[V]$ vorliegt, so erhält man eine natürliche Einbettung

$$V \subseteq \operatorname{Spek}(K[V]).$$

Einem Vektor $v \in V$ ist das maximale Ideal $\{f \in K[V] | f(v) = 0\}$ zugeordnet. Dieses wird von den in v verschwindenden Linearformen erzeugt.

Als Variante erwähnen wir noch das K-Spektrum.

Definition 13.10. Es sei K ein kommutativer Ring und R eine kommutative K-Algebra. Zu einer weiteren K-Algebra L nennt man die Menge der K-Algebrahomomorphismen

$$\operatorname{Hom}_K(R, L)$$

das *L-Spektrum* von R. Es wird mit $L-\operatorname{Spek}(R)$ bezeichnet.

Dies Bezeichnung wird insbesondere bei $L = K$ verwendet. Wenn man zu einer K-Algebra R das affine Schema als $X = \operatorname{Spek}(R)$ bezeichnet, so schreibt man auch $X(L)$ für das L-Spektrum und spricht von der Menge der *L-wertigen Punkte*. Wenn K ein algebraisch abgeschlossener Körper und R vom endlichen Typ über K ist, so besteht $X(K)$ genau aus den maximalen Idealen von R.

13. Arbeitsblatt

Aufwärmaufgaben

Aufgabe 13.1. Sei R ein kommutativer Ring und $\mathfrak{p}$ ein Ideal. Genau dann ist $\mathfrak{p}$ ein Primideal, wenn der Restklassenring $R/\mathfrak{p}$ ein Integritätsbereich ist.

Aufgabe 13.2. Sei $\mathfrak{a}$ ein Ideal in einem kommutativen Ring R. Zeige, dass $\mathfrak{a}$ genau dann ein Primideal ist, wenn $\mathfrak{a}$ der Kern eines Ringhomomorphismus $\varphi\colon R \to K$ in einen Körper K ist.

Aufgabe 13.3. Zeige, dass ein Primideal ein Radikal ist.

Aufgabe 13.4. Es sei R ein kommutativer Ring und $I \subseteq R$ ein Ideal in R. Zeige, dass I genau dann ein maximales Ideal ist, wenn der Restklassenring R/I ein Körper ist.

Aufgabe 13.5. Seien R ein kommutativer Ring und sei $\mathfrak{a} \neq R$ ein Ideal in R. Zeige: $\mathfrak{a}$ ist ein maximales Ideal genau dann, wenn es zu jedem $g \in R$, $g \notin \mathfrak{a}$, ein $f \in \mathfrak{a}$ und ein $r \in R$ gibt mit $rg + f = 1$.

Zeige (ohne Betrachtung von Restklassenringen), dass ein maximales Ideal ein Primideal ist.

Aufgabe 13.6. Sei R ein vom Nullring verschiedener kommutativer Ring. Zeige unter Verwendung des Lemmas von Zorn, dass es maximale Ideale in R gibt.

Aufgabe 13.7. Es sei R ein kommutativer Ring, $\mathfrak{a} \subseteq R$ ein Ideal und $M \subseteq R$ ein multiplikatives System mit $\mathfrak{a} \cap M = \emptyset$. Zeige mit dem Lemma von Zorn, dasss es dann auch ein Primideal $\mathfrak{p}$ mit $\mathfrak{a} \subseteq \mathfrak{p}$ und mit $\mathfrak{p} \cap M = \emptyset$ gibt.

Aufgabe 13.8. Sei $\mathfrak{a}$ ein Radikal in einem kommutativen Ring. Zeige, dass $\mathfrak{a}$ der Durchschnitt von Primidealen ist.

Vor den nächsten Aufgaben erinnern wir an den Begriff eines *lokalen Ringes* und einer Lokalisierung.

Ein kommutativer Ring R heißt *lokal*, wenn R genau ein maximales Ideal besitzt.

Sei R ein kommutativer Ring und sei $\mathfrak{p}$ ein Primideal. Dann nennt man die Nenneraufnahme an $S = R \setminus \mathfrak{p}$ die *Lokalisierung* von R an $\mathfrak{p}$. Man schreibt dafür $R_{\mathfrak{p}}$. Es ist also

$$R_{\mathfrak{p}} := \left\{ \frac{f}{g} | \, f \in R, \, g \notin \mathfrak{p} \right\} .$$

Aufgabe 13.9. Sei R ein kommutativer Ring. Zeige, dass R genau dann ein lokaler Ring ist, wenn $a + b$ nur dann eine Einheit ist, wenn a oder b eine Einheit ist.

Aufgabe 13.10. Sei R ein kommutativer Ring und sei $\mathfrak{m}$ ein maximales Ideal mit Lokalisierung $R_{\mathfrak{m}}$. Es sei $\mathfrak{a}$ ein Ideal, dass unter der Lokalisierungsabbildung zum Kern gehört. Zeige, dass dann $R_{\mathfrak{m}}$ auch eine Lokalisierung von $R/\mathfrak{a}$ ist.

Aufgabe 13.11. Beschreibe das Spektrum eines diskreten Bewertungsringes.

Aufgabe 13.12. Sei K ein Körper. Beschreibe das Spektrum von

$$K[X,Y]/(XY)\,.$$

Aufgaben zum Abgeben

Aufgabe 13.13. (3 Punkte)

Sei R ein kommutativer Ring, sei $f \in R$ und sei $\mathfrak{a}$ ein Ideal. Zeige, dass $f \in \mathfrak{a}$ genau dann gilt, wenn für alle Lokalisierungen $R_{\mathfrak{p}}$ gilt, dass $f \in \mathfrak{a}R_{\mathfrak{p}}$ ist.

Aufgabe 13.14. (5 Punkte)

Sei R ein kommutativer Ring und sei $\mathfrak{p}$ ein Primideal. Dann ist der Restklassenring $S = R/\mathfrak{p}$ ein Integritätsbereich mit Quotientenkörper $Q = Q(S)$ und $R_{\mathfrak{p}}$ ist ein lokaler Ring mit dem maximalen Ideal $\mathfrak{p}R_{\mathfrak{p}}$. Zeige, dass eine natürliche Isomorphie

$$Q(S) \cong R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$$

vorliegt.

Den in der vorstehenden Aufgabe auf zweifache Weise konstruierten Körper nennt man auch den *Restekörper* in $\mathfrak{p}$. Er wird mit $\kappa(\mathfrak{p})$ bezeichnet.

14. Vorlesung - Das Spektrum II

Funktorielle Eigenschaften des Spektrums

Das Spektrum ordnet nicht nur einem kommutativen Ring einen topologischen Raum zu, sondern auch einem Ringhomomorphismus eine stetige Abbildung zu.

Proposition 14.1. *Es sei*

$$\varphi\colon\ R \longrightarrow S$$

ein Ringhomomorphismus zwischen zwei kommutativen Ringen. Dann gelten folgende Aussagen.

(1) *Die Zuordnung*

$$\varphi^*\colon\ \operatorname{Spek}(S) \longrightarrow \operatorname{Spek}(R)\,,\ \mathfrak{p} \longmapsto \varphi^*(\mathfrak{p}) := \varphi^{-1}(\mathfrak{p}),$$

ist (wohldefiniert und) stetig.

(2) *Es ist* $(\varphi^*)^{-1}(D(\mathfrak{a})) = D(\mathfrak{a}S)$ *für jedes Ideal* $\mathfrak{a} \subseteq R$.

(3) *Für einen weiteren Ringhomomorphismus*

$$\psi\colon\ S \longrightarrow T$$

gilt $(\psi \circ \varphi)^* = \varphi^* \circ \psi^*$.

Beweis. Die Abbildung ist nach Aufgabe 14.1 wohldefiniert. Zur Stetigkeit ist die Aussage (2) zu zeigen. Wir argumentieren mit den abgeschlossenen Mengen. Für ein Primideal $\mathfrak{q} \in \operatorname{Spek}(S)$ ist $\varphi^*(\mathfrak{q}) \in V(\mathfrak{a})$ genau dann, wenn $\mathfrak{a} \subseteq \varphi^{-1}(\mathfrak{q})$ ist. Dies ist äquivalent zu $\varphi(\mathfrak{a}) \subseteq \mathfrak{q}$ und ebenso zu $\mathfrak{a}S \subseteq \mathfrak{q}$. (3) ist klar. □

Die in der vorstehenden Aussage eingeführte stetige Abbildung heißt *Spektrumsabbildung* (zu dem gegebenen Ringhomomorphismus). Bei einem Unterring $R \subseteq S$ geht es einfach um die Zuordnung $\mathfrak{p} \mapsto \mathfrak{p} \cap R$. In diesem Fall spricht man auch von „Runterschneiden“. Vor der nächsten Aussage erinnern wir an einige topologische Eigenschaften von stetigen Abbildungen. Eine stetige Abbildung

$$f : X \longrightarrow Y$$

zwischen topologischen Räumen X und Y heißt *abgeschlossen* (*offen*), wenn Bilder von abgeschlossenen (offenen) Mengen wieder abgeschlossen (offen) sind. Unter einer Einbettung versteht man eine injektive Abbildung, bei der die eingebettete Menge homöomorph zur Bildmenge ist.

Proposition 14.2. *Es sei R ein kommutativer Ring. Dann gelten folgende Aussagen.*

(1) *Zu einem Ideal $\mathfrak{a} \subseteq R$ und der Restklassenabbildung*

$$q\colon\ R \longrightarrow R/\mathfrak{a}$$

ist die Spektrumsabbildung

$$q^*\colon\ \operatorname{Spek}(R/\mathfrak{a}) \longrightarrow \operatorname{Spek}(R)$$

eine abgeschlossene Einbettung, deren Bild $V(\mathfrak{a})$ ist.

(2) *Zu einem multiplikativen System $M \subseteq R$ ist die zur kanonischen Abbildung*

$$\iota\colon\ R \longrightarrow R_M$$

gehörige Abbildung

$$\iota^*\colon\ \operatorname{Spek}(R_M) \longrightarrow \operatorname{Spek}(R)$$

injektiv, und das Bild besteht aus der Menge der Primideale von R, die zu M disjunkt sind.

(3) *Zu $f \in R$ ist die zur kanonischen Abbildung*

$$\iota\colon\ R \longrightarrow R_f$$

gehörige Abbildung

$$\iota^*\colon\ \operatorname{Spek}(R_f) \longrightarrow \operatorname{Spek}(R)$$

eine offene Einbettung, deren Bild gleich $D(f)$ ist.

Beweis. (1) folgt aus Aufgabe 10.10: Die Primideale in $R/\mathfrak{a}$ entsprechen über $\mathfrak{p} \mapsto q^{-1}(\mathfrak{p}) = \mathfrak{p} + \mathfrak{a}$ den Primidealen von R, die $\mathfrak{a}$ enthalten. Die angegebene Abbildung ist also bijektiv und hat das beschriebene Bild. Zu einem Ideal $\mathfrak{b} \subseteq R/\mathfrak{a}$ und einem Primideal $\mathfrak{p} \subseteq R/\mathfrak{a}$ ist $\mathfrak{b} \subseteq \mathfrak{p}$ genau dann, wenn

$$\mathfrak{b} + \mathfrak{a} = q^{-1}(\mathfrak{b}) \subseteq \mathfrak{p} + \mathfrak{a}$$

gilt. Also ist das Bild von $V(\mathfrak{b})$ gleich $V(\mathfrak{b}+\mathfrak{a})$ und damit abgeschlossen. Für (2) siehe Aufgabe 14.2. (3). Da für ein Primideal $\mathfrak{p}$ und ein Element $f \in R$ die Beziehung $f \notin \mathfrak{p}$ genau dann gilt, wenn $\mathfrak{p}$ zum multiplikativen System $\{f^n | \, n \in \mathbb{N}\}$ disjunkt ist, folgt aus Teil (2), dass die Abbildung injektiv ist und dass ihr Bild gleich $D(f)$ ist. Das gleiche Argument, angewendet auf $g \in R$ bzw. $\frac{g}{1} \in R_f$ zeigt, dass das Bild von $D(g) \subseteq \operatorname{Spek}(R_f)$ gleich $D(fg)$ und damit offen ist. □

Lemma 14.3. *Es sei*

$$\varphi\colon\ R \longrightarrow S$$

ein Ringhomomorphismus zwischen zwei kommutativen Ringen und es sei

$$\varphi^*\colon\ \operatorname{Spek}(S) \longrightarrow \operatorname{Spek}(R)\,,\ \mathfrak{p} \longmapsto \varphi^*(\mathfrak{p}),$$

die zugehörige Spektrumsabbildung. Dann ist die Faser über einem Primideal $\mathfrak{q} \in \operatorname{Spek}(R)$ gleich $\operatorname{Spek}\left((S/\mathfrak{q}S)_{\varphi(R\setminus\mathfrak{q})}\right)$. D.h. die Faser besteht aus allen Primidealen $\mathfrak{p} \in \operatorname{Spek}(S)$ mit $\mathfrak{q}S \subseteq \mathfrak{p}$ und mit $\mathfrak{p} \cap \varphi(R \setminus \mathfrak{q}) = \emptyset$.

Beweis. Aufgrund von Proposition 14.2 müssen wir nur die zweite Formulierung beweisen. Für ein Primideal $\mathfrak{p} \subseteq S$ gilt $\varphi^{-1}(\mathfrak{p}) = \mathfrak{q}$ genau dann, wenn sowohl $\varphi(\mathfrak{q}) \subseteq \mathfrak{p}$ als auch $\varphi(R \setminus \mathfrak{q}) \subseteq S \setminus \mathfrak{p}$ gilt. Die erste Bedingung ist zu $\mathfrak{q}S \subseteq \mathfrak{p}$ und die zweite Bedingung ist zu

$$\varphi(R \setminus \mathfrak{q}) \cap \mathfrak{p} = \emptyset$$

äquivalent. □

Insbesondere ist die Faser eines Spektrumsmorphismus über einem Punkt selbst wieder das Spektrum eines Ringes. Wir werden später eine weitere Beschreibung der Faser mit Hilfe des Tensorprodukts kennenlernen. Ein Spezialfall der vorstehenden Aussage ist, dass die Faser über einem maximalen Ideal $\mathfrak{m}$ gleich $\operatorname{Spek}(S/\mathfrak{m}S)$ ist, da in diesem Fall aus $\mathfrak{m}S \subseteq \mathfrak{p}$ sofort $\mathfrak{m} \subseteq \varphi^{-1}(\mathfrak{p})$ folgt und wegen der Maximalität Gleichheit gelten muss. Bei einem Integritätsbereich R und dem Nullideal erübrigt es sich, das Erweiterungsideal zu betrachten, die Faser wird einfach durch $\operatorname{Spek}\left(S_{\varphi(R\setminus\{0\})}\right)$ beschrieben.

Korollar 14.4. *Es sei*

$$\varphi\colon\ R \longrightarrow S$$

ein Ringhomomorphismus zwischen zwei kommutativen Ringen und es sei

$$\varphi^*\colon\ \operatorname{Spek}(S) \longrightarrow \operatorname{Spek}(R)\,,\ \mathfrak{p} \longmapsto \varphi^*(\mathfrak{p}),$$

die zugehörige Spektrumsabbildung. Dann ist die Faser über einem Primideal $\mathfrak{q} \in \operatorname{Spek}(R)$ *genau dann leer, wenn* $\mathfrak{q}S \cap \varphi(R \setminus \mathfrak{q}) \neq \emptyset$.

Beweis. Dies folgt aus Lemma 14.3 und Proposition 13.4 (6). □

Beispiel 14.5. Es sei K ein Körper und sei ein K-Algebrahomomorphismus

$$K[X_1, \ldots, X_n] \longrightarrow K[Y_1, \ldots, Y_m],\ X_i \longmapsto P_i,$$

gegeben. Nach Lemma 14.3 wird die Faser über einem maximalen Ideal der Form $(X_1 - a_1, \ldots, X_n - a_n)$ durch $V(P_1 - a_1, \ldots, P_n - a_n)$ beschrieben. Ein K-Punkt $(Y_1 - b_1, \ldots, Y_m - b_m)$ gehört zu dieser abgeschlossenen Menge genau dann, wenn

$$P_i(b_1, \ldots, b_m) = a_i$$

für $i = 1, \ldots, n$ ist.

Beispiel 14.6. Die Faser zu

$$\operatorname{Spek}(\mathbb{Z}[X]) \longrightarrow \operatorname{Spek}(\mathbb{Z})$$

über einem Primideal (p) zu einer Primzahl p ist nach Lemma 14.3 und Proposition 14.2 (1) gleich

$$V(p\mathbb{Z}[X]) = \operatorname{Spek}(\mathbb{Z}[X]/p\mathbb{Z}[X]) = \operatorname{Spek}(\mathbb{Z}/(p)[X]).$$

Über dem Nullideal (0) ist die Faser gleich

$$\operatorname{Spek}\left((\mathbb{Z}[X])_{\mathbb{Z}\setminus\{0\}}\right) = \operatorname{Spek}(\mathbb{Q}[X]).$$

In jedem Fall ist also die Faser gleich $\operatorname{Spek}(K[X])$, wenn K den Restekörper zum Primideal bezeichnet.

Die Spektrumsabbildung bei einer ganzen Erweiterung

Wir betrachten Besonderheiten der Spektrumsabbildung zu einer ganzen Erweiterung. Die folgende Aussage heißt die *going up*-Eigenschaft einer ganzen Erweiterung.

Lemma 14.7. *Es sei*

$$\varphi\colon R \longrightarrow S$$

ein ganzer Ringhomomorphismus. Es seien $\mathfrak{q}_0 \subseteq \mathfrak{q}_1$ *Primideale in* R *und* $\mathfrak{p}_0$ *ein Primideal in* S *mit* $\varphi^*(\mathfrak{p}_0) = \mathfrak{q}_0$. *Dann gibt es ein Primideal* $\mathfrak{p}_1 \supseteq \mathfrak{p}_0$ *in* S *mit* $\varphi^*(\mathfrak{p}_1) = \mathfrak{q}_1$.

Beweis. Wir betrachten die injektive Abbildung

$$R/\mathfrak{q}_0 \longrightarrow S/\mathfrak{p}_0,$$

die nach wie vor ganz ist. Wir können also annehmen, dass eine ganze Erweiterung $R \subseteq S$ von Integritätsbereichen vorliegt und müssen ein Primideal

$\mathfrak{p} \in \operatorname{Spek}(S)$ finden, das auf ein vorgegebenes Primideal $\mathfrak{q} \in \operatorname{Spek}(R)$ runterschneidet. Wir lokalisieren R an $\mathfrak{q}$ und S an $R \setminus \mathfrak{q} \subseteq S$, wobei die induzierte Abbildung

$$R_{\mathfrak{q}} \longrightarrow S_{R\setminus\mathfrak{q}}$$

nach wie vor ganz ist. Wir können also annehmen, dass R ein lokaler Integritätsbereich ist und $R \subseteq S$ eine ganze Erweiterung. Wir suchen ein Primideal aus S, das auf das maximale Ideal $\mathfrak{m}$ herunterschneidet. Nehmen wir an, dass die Faser über $\mathfrak{m}$ leer ist. Dann ist nach Korollar 14.4 das Erweiterungsideal $\mathfrak{m}S$ gleich dem Einheitsideal. Dann gibt es Elemente $f_1, \ldots, f_n \in \mathfrak{m}$ und $s_1, \ldots, s_n \in S$ mit $s_1 f_1 + \ldots + s_n f_n = 1$. Diese Gleichung gilt auch im Unterring $T = R[s_1, \ldots, s_n] \subseteq S$. Die Erweiterung $R \subseteq T$ ist endlich erzeugt und ganz, also nach Satz 11.10 sogar endlich. Es ist $\mathfrak{m}T = T$ und damit $T/\mathfrak{m}T = 0$. Aus dem Lemma von Nakayama folgt daraus $T = 0$, ein Widerspruch. □

Die folgende Aussage heißt die *lying over*-Eigenschaft einer injektiven ganzen Erweiterung.

Lemma 14.8. *Es sei*

$$\varphi\colon\ R \longrightarrow S$$

ein injektiver ganzer Ringhomomorphismus. Dann ist die Spektrumsabbildung

$$\varphi^*\colon\ \operatorname{Spek}(S) \longrightarrow \operatorname{Spek}(R)$$

surjektiv.

Beweis. Sei $\mathfrak{q} \in \operatorname{Spek}(R)$ vorgegeben. Die induzierte Abbildung

$$R_{\mathfrak{q}} \longrightarrow S_{R\setminus\mathfrak{q}}$$

ist ebenfalls injektiv. Der Beweis zu Lemma 14.7 zeigt, dass es ein Primideal aus $S_{R\setminus\mathfrak{q}}$ gibt, das auf $\mathfrak{q}$ runterschneidet. □

Satz 14.9. *Es seien R und S kommutative Ringe und es sei*

$$\varphi\colon\ R \longrightarrow S$$

ein ganzer Ringhomomorphismus. Dann ist die Spektrumsabbildung

$$\varphi^*\colon\ \operatorname{Spek}(S) \longrightarrow \operatorname{Spek}(R)$$

abgeschlossen. Wenn φ zusätzlich injektiv ist, so ist φ^* surjektiv.

Beweis. Wir zeigen für eine beliebige abgeschlossene Teilmenge $V(\mathfrak{a}) \subseteq \operatorname{Spek}(S)$ mit einem Ideal $\mathfrak{a} \subseteq S$, dass das Bild

$$\varphi^*(V(\mathfrak{a})) = V(\varphi^{-1}(\mathfrak{a}))$$

ist, also insbesondere wieder abgeschlossen ist. Dafür betrachten wir den induzierten Ringhomomorphismus

$$R/\varphi^{-1}(\mathfrak{a}) \longrightarrow S/\mathfrak{a},$$

der ebenfalls ganz und zusätzlich injektiv ist. Daher ist

$$V(\mathfrak{a}) \cong \operatorname{Spek}(S/\mathfrak{a}) \longrightarrow V(\varphi^{-1}(\mathfrak{a})) \cong \operatorname{Spek}\left(R/\varphi^{-1}(\mathfrak{a})\right)$$

nach Lemma 14.8 surjektiv. Also ist $\varphi^*(V(\mathfrak{a})) = V(\varphi^{-1}(\mathfrak{a}))$. Der Zusatz folgt ebenfalls aus Lemma 14.8. □

Lemma 14.10. *Es sei K ein Körper, A ein Integritätsbereich und $K \subseteq A$ eine ganze Erweiterung. Dann ist auch A ein Körper.*

Beweis. Es sei $a \in A$, $a \neq 0$. Wir betrachten eine Ganzheitsgleichung

$$a^n + r_{n-1}a^{n-1} + \ldots + r_1 a + r_0 = 0.$$

Wenn $r_0 = 0$ ist, so können wir a ausklammern und erhalten, da a ein Nichtnullteiler ist, eine Ganzheitsgleichung kleineren Grades. Wir können also annehmen, dass $r_0 \neq 0$ ist. Dann ist

$$a \cdot \left(a^{n-1} + r_{n-1}a^{n-2} + \ldots + r_1\right) \cdot \left(-r_0^{-1}\right) = 1$$

und somit ist a eine Einheit. □

Lemma 14.11. *Es sei*

$$\varphi\colon R \longrightarrow S$$

ein ganzer Ringhomomorphismus. Es seien $\mathfrak{p} \neq \mathfrak{q}$ Primideale in S mit $\varphi^*(\mathfrak{p}) = \varphi^*(\mathfrak{q})$. Dann ist $\mathfrak{p} \not\subseteq \mathfrak{q}$. D.h. die Fasern sind nulldimensional.

Beweis. Es sei $\mathfrak{r} := \varphi^*(\mathfrak{p}) = \varphi^*(\mathfrak{q})$. Wir machen den Übergang

$$R \longrightarrow R_{\mathfrak{r}}/\mathfrak{r}R_{\mathfrak{r}} = \kappa(\mathfrak{r})$$

und betrachten die induzierte Abbildung

$$\kappa(\mathfrak{r}) =: K \longrightarrow (S/\mathfrak{r}S)_{\varphi(R\setminus\mathfrak{r})} =: A,$$

die ebenfalls ganz ist. Nach Lemma 14.3 ist $\operatorname{Spek}(A)$ die Faser von φ^* über $\mathfrak{r}$. Wir müssen also zeigen, dass das Spektrum einer über einem Körper K ganzen Algebra nulldimensional ist, es also keine Inklusionen von Primidealen gibt. Sei $\mathfrak{p} \subseteq \mathfrak{q}$ eine Inklusion von Primidealen aus A. Wir gehen zu $K \to A/\mathfrak{p}$ über. Somit ist $A/\mathfrak{p}$ ein Integritätsbereich und eine ganze Erweiterung eines Körpers. Nach Lemma 14.10 ist $A/\mathfrak{p}$ selbst ein Körper. Also ist

$$\mathfrak{q} = \mathfrak{p}.$$

□

Satz 14.12. *Es sei*

$$\varphi\colon R \longrightarrow S$$

ein injektiver ganzer Ringhomomorphismus. Dann ist

$$\dim(S) = \dim(R).$$

Beweis. Zu einer Primidealkette $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \ldots \subset \mathfrak{p}_n$ aus S ist die Kette $\varphi^*(\mathfrak{p}_0) \subset \varphi^*(\mathfrak{p}_1) \subset \ldots \subset \varphi^*(\mathfrak{p}_n)$ nach Lemma 14.11 ebenfalls echt, so dass

$$\dim(S) \leq \dim(R)$$

ist. Zu einer Primidealkette $\mathfrak{q}_0 \subset \mathfrak{q}_1 \subset \ldots \subset \mathfrak{p}_n$ aus R gibt es zunächst nach Lemma 14.8 ein Primideal $\mathfrak{p}_0$ aus S mit $\varphi^*(\mathfrak{p}_0) = \mathfrak{q}_0$. Nach Lemma 14.7 kann man dies sukzessive zu einer Kette $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \ldots \subset \mathfrak{p}_n$ mit $\varphi^*(\mathfrak{p}_i) = \mathfrak{q}_i$ fortsetzen. Daher ist auch

$$\dim(S) \geq \dim(R).$$

□

Satz 14.13. *Es sei*

$$R \longrightarrow S$$

ein endlicher Ringhomomorphismus zwischen kommutativen Ringen. Dann bestehen die Fasern der Spektrumsabbildung

$$\operatorname{Spek}(S) \longrightarrow \operatorname{Spek}(R)$$

aus endlich vielen Punkten.

Beweis. Siehe Aufgabe 14.16. □

14. Arbeitsblatt

Aufwärmaufgaben

Aufgabe 14.1. Seien R und S kommutative Ringe und sei $\varphi : R \to S$ ein Ringhomomorphismus. Sei $\mathfrak{p}$ ein Primideal in S. Zeige, dass das Urbild $\varphi^{-1}(\mathfrak{p})$ ein Primideal in R ist.

Zeige durch ein Beispiel, dass das Urbild eines maximalen Ideales kein maximales Ideal sein muss.

Aufgabe 14.2. Sei R ein Integritätsbereich und $S \subseteq R$ ein multiplikatives System. Zeige, dass die Primideale in R_S genau denjenigen Primidealen in R entsprechen, die mit S einen leeren Durchschnitt haben.

Aufgabe 14.3. Beschreibe das Spektrum $\operatorname{Spek}(R_{\mathfrak{p}})$ einer Lokalisierung eines kommutativen Ringes R an einem Primideal $\mathfrak{p}$.

Aufgabe 14.4. Es sei

$$\varphi\colon\ R \longrightarrow S$$

ein Ringhomomorphismus zwischen den kommutativen Ringen R und S und es sei $\mathfrak{p} \in \operatorname{Spek}(S)$ ein Primideal. Zeige, dass es natürliche Ringhomomorphismen

$$R_{\varphi^{-1}(\mathfrak{p})} \longrightarrow S_{\mathfrak{p}}$$

(zwischen den Lokalisierungen) und

$$\kappa(\varphi^{-1}(\mathfrak{p})) \longrightarrow \kappa(\mathfrak{p})$$

(zwischen den Restekörpern) gibt.

Aufgabe 14.5.*

Sei K ein Körper und seien R und S integre, endlich erzeugte K-Algebren. Es sei

$$\varphi : R \longrightarrow S$$

ein K-Algebrahomomorphismus und $\mathfrak{n}$ ein maximales Ideal in S mit $\varphi^{-1}(\mathfrak{n}) = \mathfrak{m}$. Die Abbildung induziere einen Isomorphismus $R_{\mathfrak{m}} \to S_{\mathfrak{n}}$. Zeige, dass es dann auch ein $f \in R$, $f \notin \mathfrak{m}$, gibt derart, dass $R_f \to S_{\varphi(f)}$ ein Isomorphismus ist.

Aufgabe 14.6. Zeige, dass die Spektrumsabbildung zur Reduktion

$$R \longrightarrow R/\mathfrak{n}_R$$

eines kommutativen Ringes R eine Homöomorphie ist.

Aufgabe 14.7. Sei R ein kommutativer Ring, der einen Körper der positiven Charakteristik $p > 0$ enthalte (dabei ist p eine Primzahl). Zeige, dass die Abbildung

$$R \longrightarrow R,\ f \longmapsto f^p,$$

ein Ringhomomorphismus ist, den man den *Frobenius-Homomorphismus* nennt.

Aufgabe 14.8. Es sei R ein kommutativer Ring der positiven Charakteristik $p > 0$. Zeige, dass die Spektrumsabbildung zum Frobenius-Homomorphismus

$$R \longrightarrow R,\ f \longmapsto f^p,$$

eine Homöomorphie ist.

Aufgabe 14.9. Es sei R ein kommutativer Ring. Bestimme die Fasern zur Spektrumsabbildung zur Ringerweiterung $R \subseteq R[X_1, \ldots, X_n]$.

Aufgabe 14.10. Bestimme die Fasern der Spektrumsabbildung zu $\mathbb{R}[X] \subseteq \mathbb{C}[X]$.

Wenn der Grundkörper die komplexen Zahlen sind, so gibt es auf dem $\mathbb{C}$-Spektrum auch eine komplexe Topologie, die wesentlich feiner als die Zariski-Topologie ist. Dies wird in den folgenden Aufgaben entwickelt.

Aufgabe 14.11. Es sei R eine endlich erzeugte kommutative $\mathbb{C}$-Algebra. Zeige, dass es auf dem $\mathbb{C}$-Spektrum $\mathbb{C}-\mathrm{Spek}\,(R)$ eine *natürliche Topologie* (oder *komplexe Topologie*) gibt, die im Falle des Polynomringes $\mathbb{C}[X_1, \ldots, X_n]$ mit der metrischen Topologie auf dem $\mathbb{C}^n$ übereinstimmt. Zeige ferner, dass zu einem $\mathbb{C}$-Algebrahomomorphismus $\varphi\colon\ R \to S$ zwischen endlich erzeugten $\mathbb{C}$-Algebren R und S die induzierte Abbildung

$$\mathbb{C}-\mathrm{Spek}\,(S) \longrightarrow \mathbb{C}-\mathrm{Spek}\,(R)$$

stetig in der natürlichen Topologie ist.

Aufgabe 14.12. Es sei $P \in \mathbb{C}[X]$ ein nichtkonstantes Polynom. Zeige, dass die Funktion

$$\mathbb{C} \longrightarrow \mathbb{C},\ z \longmapsto P(z),$$

die Eigenschaft besitzt, dass Urbilder von beschränkten Teilmengen $T \subseteq \mathbb{C}$ beschränkt sind.

Aufgabe 14.13. Es seien $F_1, \ldots, F_k \in \mathbb{C}[X_1, \ldots, X_n]$ Polynome mit der Eigenschaft, dass der dadurch definierte $\mathbb{C}$-Algebrahomomorphismus

$$\mathbb{C}[Y_1, \ldots, Y_k] \longrightarrow \mathbb{C}[X_1, \ldots, X_n],\ Y_j \longmapsto F_j,$$

ganz ist. Zeige, dass die zugehörige Abbildung

$$\mathbb{C}^n \longrightarrow \mathbb{C}^k,\ (x_1, \ldots, x_n) \longmapsto (F_1(x_1, \ldots, x_n), \ldots, F_k(x_1, \ldots, x_n)),$$

die Eigenschaft besitzt, dass Urbilder von beschränkten Teilmengen $T \subseteq \mathbb{C}^k$ wieder beschränkt sind.

Man folgere, dass in der vorstehenden Situation die Abbildung F eigentlich ist, dass also Urbilder kompakter Teilmengen wieder kompakt sind, und dass F abgeschlossen ist.

Aufgaben zum Abgeben

Aufgabe 14.14. (3 Punkte)

Zeige, dass bei $R \subset R[X]$ die going-up-Eigenschaft nicht gelten muss.

Aufgabe 14.15. (3 Punkte)

Zeige, dass die Spektrumsabbildung zur Normalisierung einer monomialen Kurve eine Homöomorphie ist.

Aufgabe 14.16. (3 Punkte)

Es sei $R \to S$ ein endlicher Ringhomomorphismus zwischen kommutativen Ringen. Zeige, dass die Fasern der Spektrumsabbildung

$$\operatorname{Spek}(S) \longrightarrow \operatorname{Spek}(R)$$

aus endlich vielen Punkten bestehen.

Aufgabe 14.17. (5 Punkte)

Bestimme die Fasern der Spektrumsabbildung zu $\mathbb{Q}[X] \subseteq \mathbb{R}[X]$. Welche sind endlich?

15. Vorlesung - Quotient und Invariantenring

Operationen auf dem Spektrum

Es sei G eine Gruppe, die auf einem kommutativen Ring als Gruppe von Ringautomorphismen operiere. Zu jedem $\sigma \in G$ liegt also ein Ringautomorphismus

$$\varphi_\sigma \colon R \longrightarrow R$$

vor, der wiederum zu einer Spektrumsabbildung

$$\varphi_\sigma^* \colon \operatorname{Spek}(R) \longrightarrow \operatorname{Spek}(R)$$

führt, die eine Homöomorphie ist. Die Operation von G auf R ergibt als eine Operation von G auf $\operatorname{Spek}(R)$ als Gruppe von Homöomorphismen. Da wir die Operation auf dem Ring von rechts schreiben, und das Spektrum kontravariant ist, ist es natürlich, die Operation auf dem affinen Schema von links zu schreiben. Wir werden gleich sehen, dass man bei einer linearen Operation auf einem Vektorraum und der zugehörigen Operation auf dem Polynomring über das Spektrum die ursprüngliche Operation zurückgewinnt.

Lemma 15.1. *Es sei K ein Körper und V und W seien zwei endlichdimensionale K-Vektorräume. Es sei*

$$\psi \colon V \longrightarrow W$$

eine K-lineare Abbildung und

$$\varphi \colon K[W] \longrightarrow K[V]$$

der zugehörige K-Algebrahomomorphismus zwischen den Polynomringen und

$$\varphi^* \colon \operatorname{Spek}(K[V]) \longrightarrow \operatorname{Spek}(K[W])$$

die zugehörige Spektrumsabbildung. Dann kommutiert das Diagramm

$$\begin{array}{ccc} V & \stackrel{\psi}{\longrightarrow} & W \\ \downarrow & & \downarrow \\ \operatorname{Spek}(K[V]) & \stackrel{\varphi^*}{\longrightarrow} & \operatorname{Spek}(K[W]) \end{array},$$

wobei die vertikalen Abbildungen die natürlichen Einbettungen sind.

Beweis. Es seien $\mathfrak{m}_v = \{F \in K[V] | F(v) = 0\}$ und $\mathfrak{m}_w = \{G \in K[W] | G(w) = 0\}$ die zu den Vektoren v bzw. w gehörigen maximalen Ideale. Die Aussage folgt aus

$$\begin{aligned} \varphi^*(\mathfrak{m}_v) &= \varphi^{-1}(\mathfrak{m}_v) \\ &= \{G \in K[W] | \varphi(G) \in \mathfrak{m}_v\} \\ &= \{G \in K[W] | \varphi(G)(v) = 0\} \\ &= \{G \in K[W] | (G \circ \psi)(v) = 0\} \\ &= \{G \in K[W] | G(\psi(v)) = 0\} \\ &= \mathfrak{m}_{\psi(v)}. \end{aligned}$$

□

Proposition 15.2. *Es sei K ein Körper, V ein endlichdimensionaler K-Vektorraum, auf dem eine Gruppe G linear operiere. Es sei*

$$K[V] \times G \longrightarrow K[V]$$

die zugehörige Operation auf dem Polynomring $K[V]$ und

$$G \times \operatorname{Spek}(K[V]) \longrightarrow \operatorname{Spek}(K[V])$$

die zugehörige Operation auf dem Spektrum. Dann liegt über die natürliche Einbettung $V \subseteq \operatorname{Spek}(K[V])$ eine Fortsetzung der Operation vor.

Beweis. Dies folgt unmittelbar aus Lemma 15.1. □

Quotient und Invariantenring bei endlichen Gruppen

Es sei R ein kommutativer Ring, G eine endliche Gruppe, die auf R und damit auch auf $X = \operatorname{Spek}(R)$ als Gruppe von Automorphismen operiere. Dann hat man einerseits den topologischen Quotienten X/G und andererseits den Invariantenring R^G und damit dessen Spektrum $\operatorname{Spek}\left(R^G\right)$. Wir zeigen nach einigen Vorbereitungen, dass diese zwei geometrischen Objekte gleich sind, also dass

$$X/G = \operatorname{Spek}\left(R^G\right)$$

gilt. Dabei werden wir zeigen, dass die Spektrumsabbildung

$$\iota^*\colon \operatorname{Spek}(R) \longrightarrow \operatorname{Spek}\left(R^G\right)$$

(die zur Inklusion $R^G \subseteq R$ gehört) die Eigenschaften eines topologischen Quotienten erfüllt.

Korollar 15.3. *Es sei R ein kommutativer Ring, auf dem eine endliche Gruppe G durch Ringautomorphismen operiere. Dann ist die Spektrumsabbildung*

$$\iota^*\colon\ \mathrm{Spek}\,(R) \longrightarrow \mathrm{Spek}\left(R^G\right)$$

surjektiv und abgeschlossen. Insbesondere trägt $\mathrm{Spek}\left(R^G\right)$ *die Bildtopologie unter dieser Abbildung.*

Beweis. Dies folgt aus Lemma 12.1 und aus Satz 14.9. □

Für die nächste Aussage über die Fasern und Bahnen bei einer endlichen Gruppenoperation benötigen wir das Lemma über die *Primvermeidung*.

Lemma 15.4. *Es sei R ein kommutativer Ring, $\mathfrak{a}$ ein Ideal und $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ eine endliche Familie von Primidealen. Es gelte $\mathfrak{a} \subseteq \bigcup_{i=1}^n \mathfrak{p}_i$. Dann ist $\mathfrak{a} \subseteq \mathfrak{p}_i$ für ein i.*

Beweis. Wir führen Induktion über n. Bei $i = 1$ ist die Aussage trivial. Sei die Aussage für n Primideale bewiesen, und seien $n+1$ Primideale gegeben. Für jedes i können wir annehmen, dass $\mathfrak{a} \not\subseteq \bigcup_{j\neq i} \mathfrak{p}_j$ ist, da anderfalls die Aussage nach Induktionsvoraussetzung bewiesen ist. Demnach gibt es jeweils ein $f_i \in \mathfrak{a}$ mit $f_i \notin \bigcup_{j\neq i} \mathfrak{p}_j$. Dann muss insbesondere $f_i \in \mathfrak{p}_i$ sein. Das Element $f_1 + f_2 f_3 \cdots f_{n+1}$ gehört zu $\mathfrak{a}$ und damit ist auch $f_1 + f_2 f_3 \cdots f_{n+1} \in \mathfrak{p}_i$ für ein i. Dies ist aber sowohl bei $i = 1$ als auch bei $i \geq 2$ ein Widerspruch. □

Lemma 15.5. *Es sei R ein kommutativer Ring, auf dem eine endliche Gruppe G durch Ringautomorphismen operiere und es sei*

$$\iota^*\colon\ \mathrm{Spek}\,(R) \longrightarrow \mathrm{Spek}\left(R^G\right)$$

die zugehörige Spektrumsabbildung. Dann gilt für $\mathfrak{p}, \mathfrak{q} \in \mathrm{Spek}\,(R)$ die Äquivalenz: $\iota^*(\mathfrak{p}) = \iota^*(\mathfrak{q})$ genau dann, wenn es ein $\sigma \in G$ gibt mit $\sigma^*(\mathfrak{p}) = \mathfrak{q}$. Das heißt, dass die Bahnen der Operation von G auf $\mathrm{Spek}\,(R)$ *mit den Fasern von ι^* übereinstimmen.*

Beweis. Wenn $\sigma^*(\mathfrak{p}) = \sigma^{-1}(\mathfrak{p}) = \mathfrak{q}$ ist und $f \in R^G \cap \mathfrak{q}$, so ist auch $f = \sigma(f) \in \mathfrak{p}$, also ist

$$\iota^*(\mathfrak{p}) \;=\; R^G \cap \mathfrak{p} \;=\; R^G \cap \mathfrak{q} \;=\; \iota^*(\mathfrak{q}).$$

Primideale in derselben Bahn besitzen also den gleichen Bildpunkt unter der Spektrumsabbildung.

Zum Beweis der Umkehrung betrachten wir die Faser über $\mathfrak{r} \in \mathrm{Spek}\left(R^G\right)$ und es sei $\mathfrak{p}$ ein Element dieser Faser, welches es nach Korollar 15.3 gibt. Wir müssen zeigen, dass jedes Primideal $\mathfrak{q}$ der Faser in der Bahn durch $\mathfrak{p}$ liegt, dass es also ein $\sigma \in G$ gibt mit $\sigma^*(\mathfrak{p}) = \mathfrak{q}$. Wir nehmen an, dass dies nicht der Fall sei, und es sei $\mathfrak{q}$ ein Primideal der Faser, das aber nicht zur Bahn gehört. Aus $\mathfrak{q} \neq \sigma^*(\mathfrak{p})$ (für alle $\sigma \in G$) folgt $\mathfrak{q} \not\subseteq \sigma^*(\mathfrak{p})$, da andernfalls die Faser

im Widerspruch zu Lemma 14.11 nicht nulldimensional wäre. Nach Lemma 15.4 ist dann auch

$$\mathfrak{q} \not\subseteq \bigcup_{\sigma\in G} \sigma^*(\mathfrak{p}) =: T.$$

Sei $f \in \mathfrak{q}$, $f \notin T$. Die Menge T wird unter der Gruppenoperation auf sich selbst abgebildet, daher ist auch $\sigma(f) \notin T$. Somit ist auch $g = \prod_{\sigma\in G} \sigma(f) \notin T$. Andererseits ist aber $g \in R^G$ und $g \in \mathfrak{q}$, also $g \in R^G \cap \mathfrak{q} = \mathfrak{r} \subseteq \mathfrak{p} \subseteq T$. □

Satz 15.6. *Es sei R ein kommutativer Ring, auf dem eine endliche Gruppe G durch Ringautomorphismen operiere und es sei*

$$\iota^*\colon \operatorname{Spek}(R) \longrightarrow \operatorname{Spek}\left(R^G\right)$$

die zugehörige Spektrumsabbildung. Dann ist $\left(\operatorname{Spek}\left(R^G\right), \iota^*\right)$ der Quotient der Gruppenoperation von G auf $\operatorname{Spek}(R)$.

Beweis. Die Abbildung

$$\iota^*\colon \operatorname{Spek}(R) \longrightarrow \operatorname{Spek}\left(R^G\right)$$

ist nach Korollar 15.3 surjektiv, so dass nach Lemma 15.5 die Punkte aus $\operatorname{Spek}\left(R^G\right)$ den Bahnen der Gruppenoperation entsprechen. Daher ist $\operatorname{Spek}\left(R^G\right)$ ein mengentheoretischer Quotient. Nach Korollar 15.3 trägt $\operatorname{Spek}\left(R^G\right)$ die Bildtopologie, so dass es sich auch um einen topologischen Quotienten handelt. □

Aus den vorstehenden Aussagen folgt insbesondere, dass die Fasern der Spektrumsabbildung

$$\operatorname{Spek}(R) \longrightarrow \operatorname{Spek}\left(R^G\right)$$

aus endlich vielen Elementen bestehen, und zwar ist deren Anzahl maximal gleich der Anzahl der Elemente der Gruppe G.

Quotient und Invariantenring allgemein

Wenn die Gruppe nicht endlich ist, so ist das Spektrum des Invariantenringes im Allgemeinen nicht der Quotient der Gruppenoperation. Es ist ein eigenständiges, umfassendes Problem, den Quotienten zu einer algebaischen Gruppenoperation zu bestimmen, die unter der Bezeichnung *geometrische Invariantentheorie* firmiert. Zwar existiert stets der Bahnenraum, der mit der Bildtopologie versehen der Quotient in der Kategorie der topologischen Räume ist, doch wünscht man sich auch eine algebraische Struktur auf dem Quotienten (beispielsweise möchte man über „polynomiale Funktionen“ auf dem Quotienten sprechen können). Schon einfache Beispiele zeigen, dass man einen sinnvollen algebraisch-geometrischen Quotienten nur erwarten kann, wenn man die Operation auf eine offene (möglichst große) Teilmenge einschränkt. Um den Quotienten zu beschreiben reichen die affinen Varietäten

nicht aus, und nur solche kann man über Invariantenringe gewinnen. Stattdessen muss man in der Kategorie der quasiprojektiven Varietäten bzw. der Schemata einen Quotienten konstruieren.

Beispiel 15.7. Die Operation der Einheitengruppe $K^\times$ eines Körpers K auf dem K^n ($n \geq 2$) durch skalare Multiplikation besitzt den Nullpunkt als Fixpunkt und die Geraden durch den Nullpunkt ohne diesen als weitere Bahnen. Die zugehörige Operation auf dem Polynomring $R = K[X_1, \ldots, X_n]$ (vergleiche Beispiel 5.9) besitzt bei unendlichem K nur die Konstanten als invariante Polynome. Die Spektrumsabbildung

$$\operatorname{Spek}(R) \longrightarrow \operatorname{Spek}\left(R^G\right)$$

ist also konstant und vermag nicht die Bahnen zu trennen. Nach Aufgabe 5.12 gibt es bei $K = \mathbb{R}$ (oder $\mathbb{C}$) noch nicht einmal stetige Funktionen des $\mathbb{R}^n$ in einen metrischen Raum, die die Bahnen trennen.

Wenn man hingegen den Nullpunkt herausnimmt, so ist der Bahnenraum nach Definition der projektive Raum über K, einer der wichtigsten Räume überhaupt. Dieser ist nicht das Spektrum eines kommutativen Ringes, er wird aber überdeckt durch offene Teilmengen, die Spektren zu kommutativen Ringen sind. Ein solches geometrisches Objekt nennt man ein *Schema*. Die skalare Multiplikation auf dem punktierten affinen Raum besitzt also einen sinnvollen Quotienten in der Kategorie der Schemata.

Dennoch besitzt das Spektrum des Invariantenringes viele Eigenschaften, die man auch von einem Quotienten erwartet. Z.B. ist die Spektrumsabbildung

$$\operatorname{Spec} R \longrightarrow \operatorname{Spec} R^G$$

surjektiv, wenn R^G ein direkter Summand in R ist, wenn also ein Reynolds-Operator existiert. Dies ist nicht nur bei endlichen (nicht modularen) Gruppen der Fall, sondern auch bei diagonalisierbaren Operationen, die den Graduierungen entsprechen, und allgemeiner bei den sogenannten linear-reduktiven Gruppen, die wir später einführen werden.

Lemma 15.8. *Es seien R, S kommutative Ringe und $R \subseteq S$ ein direkter Summand. Dann ist die Spektrumsabbildung*

$$\operatorname{Spek}(S) \longrightarrow \operatorname{Spek}(R)$$

surjektiv.

Beweis. Es sei

$$S \cong R \oplus V$$

mit einem R-Modul V. Es sei $\mathfrak{p}$ ein Primideal von R. Nach Aufgabe 6.11 und nach Aufgabe 6.12 sind auch

$$R_{\mathfrak{p}} \longrightarrow S_{R\setminus\mathfrak{p}} = R_{\mathfrak{p}} \oplus V_{\mathfrak{p}}$$

und

$$\kappa(\mathfrak{p}) = R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}} \longrightarrow S_{R\setminus\mathfrak{p}}/\left(\mathfrak{p}R_{\mathfrak{p}}\right) S_{R\setminus\mathfrak{p}} = R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}} \oplus V_{\mathfrak{p}}/\mathfrak{p}V_{\mathfrak{p}}$$

direkte Summanden. Daher ist insbesondere der Ring rechts nicht 0 und somit ist nach Proposition 13.4 (6) und nach Korollar 14.4 die Faser über $\mathfrak{p}$ nicht leer. □

Das folgende Beispiel, das an Beispiel 6.9 anschließt, zeigt, dass die Spektrumsabbildung zum Invariantenring zu einer Operation der additiven Gruppe $(K,+)$ nicht surjektiv sein muss.

Beispiel 15.9. Es sei K ein Körper der Charakteristik 0 und $A = K[X,Y]$. Auf der A-Algebra

$$B \;=\; A[S,T]/(XS+YT+1) \;=\; K[X,Y,S,T]/(XS+YT+1)$$

operiert die additive Gruppe $(K,+)$, indem ein $\lambda \in K$ durch

$$X \mapsto X,\; Y \mapsto Y,\; S \mapsto S+\lambda Y,\; T \mapsto T-\lambda X$$

wirkt. Wie in Beispiel 6.9 gezeigt wurde, ist der Invariantenring unter dieser Gruppenoperation gleich $A = K[X,Y]$. Die Spektrumsabbildung

$$\operatorname{Spek}(B) \longrightarrow \operatorname{Spek}(A)$$

ist nicht surjektiv. Für das maximale Ideal

$$\mathfrak{m} \;=\; (X,Y) \;\subset\; A$$

ist das Erweiterungsideal $(X,Y)B$ offenbar gleich dem Einheitsideal. Somit ist die Faser über $\mathfrak{m}$ nach Korollar 14.4 leer. Zu jedem anderen Primideal $\mathfrak{p} \in \operatorname{Spek}(A)$, $\mathfrak{p} \neq \mathfrak{m}$ ist die Faser gleich $\kappa(\mathfrak{p})[S,T]/(\psi(X)S+\psi(Y)T+1)$, wobei

$$\psi\colon\; A = K[X,Y] \longrightarrow \kappa(\mathfrak{p})$$

der kanonische Ringhomomorphismus in den Restekörper ist. Nach Voraussetzung ist mindestens eines der $\psi(X), \psi(Y)$ eine Einheit, so dass eine Isomorphie zu $\kappa(\mathfrak{p})[U]$ vorliegt. Die Fasern sind also affine Geraden. Diese sind wiederum genau die Bahnen der Operation, so dass die offene Teilmenge

$$D(\mathfrak{m}) \subset \operatorname{Spek}(A)$$

der Quotient der Operation ist.

15. Arbeitsblatt

Aufwärmaufgaben

Aufgabe 15.1. Es sei G eine Gruppe, die auf einem Integritätsbereich R als Gruppe von Ringautomorphismen operiere. Zeige, dass das Nullideal $(0) \in \operatorname{Spek}(R)$ ein Fixpunkt der Operation von G auf dem Spektrum ist.

Aufgabe 15.2. Es sei K ein Körper der Charakteristik $\neq 2$. Wir betrachten die Operation von $\mathbb{Z}/(2)$ auf $\operatorname{Spek}(K[T])$, wobei das nichttriviale Element durch $T \mapsto -T$ operieren möge. Bestimme die Fixpunkte dieser Operation.

Aufgabe 15.3. Bestimme die Fixpunkte der Operationen auf $\operatorname{Spek}(\mathbb{C}[X,Y])$, die durch folgende Untergruppen G der $\mathrm{GL}_2(\mathbb{C})$ gegeben sind.

(1) $G = \mathrm{GL}_2(\mathbb{C})$,
(2) $G = \mathrm{SL}_2(\mathbb{C})$,
(3) $G = \mathbb{C}^\times = \mathbb{C}^\times \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.
(4) G die Gruppe der invertierbaren Diagonalmatrizen.
(5) G die Gruppe der reellen Drehmatrizen.

Aufgabe 15.4. Es sei G eine Gruppe, die auf einem kommutativen Ring R als Gruppe von Ringautomorphismen und damit auf $\operatorname{Spek}(R)$ operiere. Es sei $\mathfrak{p} \in \operatorname{Spek}(R)$. Zeige, dass der Stabilisator $G_{\mathfrak{p}}$ auf dem lokalen Ring $R_{\mathfrak{p}}$ und auf dem Restekörper $\kappa(\mathfrak{p})$ in natürlicher Weise operiert.

Aufgabe 15.5. Es sei K ein algebraisch abgeschlossener Körper und R eine endlich erzeugte kommutative K-Algebra. Es sei G eine Gruppe, die auf R als Gruppe von K-Algebraautomorphismen operiere. Es sei $\mathfrak{m} \in \operatorname{Spek}(R)$ ein maximales Ideal, das unter der zugehörigen Gruppenoperation auf $\operatorname{Spek}(R)$ ein Fixpunkt sei. Zeige, dass die nach Aufgabe 15.1 zugehörige Operation von G auf dem Restekörper $\kappa(\mathfrak{m})$ trivial ist.

Eine Operation einer Gruppe G auf einer Menge M heißt *fixpunktfrei*, wenn für jedes $g \in G$, $g \neq e$, die Abbildung

$$M \longrightarrow M,\ x \longmapsto gx,$$

fixpunktfrei ist.

Aufgabe 15.6. Zeige, dass eine Operation einer Gruppe G auf einer Menge M genau dann fixpunktfrei ist, wenn für jeden Punkt $x \in M$ der Stabilisator G_x trivial ist.

Eine Gruppenoperation auf einem Spektrum ist in den seltensten Fällen fixpunktfrei im strengen Sinne der obigen Definition. Häufig kann man aber die Operation auf eine offene Teilmenge derart einschränken, dass sie auf den maximalen Idealen dieser offenen Menge fixpunktfrei ist.

Aufgabe 15.7. Wir betrachten die natürliche Operation der symmetrischen Gruppe S_n auf dem K^n, wobei K einen Körper der Charakteristik $\neq 2$ bezeichne. Bestimme die größte Teilmenge $U \subseteq K^n$ derart, dass S_n auf U fixpunktfrei operiert.

Aufgabe 15.8. Es sei K ein Körper der Charakteristik $\neq 2$. Wir betrachten die natürliche Operation der symmetrischen Gruppe S_n auf $\operatorname{Spek}(K[T_1, \ldots, T_n])$. Bestimme die größte offene Teilmenge $U \subseteq \operatorname{Spek}(K[T_1, \ldots, T_n])$ derart, dass S_n auf der Menge der abgeschlossenen Punkte aus U fixpunktfrei operiert.

Aufgabe 15.9. Es sei

$$\sigma \colon R \longrightarrow R$$

ein Ringautomorphismus auf einem kommutativen Ring R. Wir betrachten die Menge

$$M = \{f - f\sigma \mid f \in R\}.$$

Zeige, dass M eine Untergruppe von $(R, +)$ ist, aber im Allgemeinen kein Ideal.

Aufgabe 15.10. Es sei

$$\sigma \colon R \longrightarrow R$$

ein Ringautomorphismus auf einem kommutativen Ring R. Wir setzen

$$M = \{f - f\sigma \mid f \in R\}$$

und betrachten ein Primideal $\mathfrak{p}$. Zeige, dass aus $M \subseteq \mathfrak{p}$ folgt, dass $\mathfrak{p}$ ein Fixpunkt unter der Spektrumsabbildung zu σ ist, und dass davon nicht die Umkehrung gelten muss.

Für die folgende Aufgabe ist Aufgabe 14.13 hilfreich.

Aufgabe 15.11. Es sei G eine endliche Gruppe, die auf dem $\mathbb{C}^n$ linear operiere. Es sei $S = \mathbb{C}[X_1, \ldots, X_n]^G$ der zugehörige Invariantenring. Zeige, dass der Bahnenraum $\mathbb{C}^n \backslash G$, versehen mit der Bildtopologie des (euklidischen) $\mathbb{C}^n$, mit dem $\mathbb{C}$-Spektrum $\mathbb{C}-\operatorname{Spek}(S)$, versehen mit der natürlichen Topologie, übereinstimmt.

Aufgaben zum Abgeben

Aufgabe 15.12. (3 Punkte)

Es sei G eine Gruppe, die auf einem kommutativen Ring R als Gruppe von Ringautomorphismen operiere und es sei $\mathfrak{p} \in \operatorname{Spek}(R)$ ein Primideal. Zeige, dass $\mathfrak{p}$ genau dann ein Fixpunkt der zugehörigen Operation auf $\operatorname{Spek}(R)$ ist, wenn die abgeschlossene Teilmenge $V(\mathfrak{p})$ G-invariant ist.

Aufgabe 15.13. (4 Punkte)

Es sei K ein algebraisch abgeschlossener Körper und R eine endlich erzeugte kommutative K-Algebra. Es sei

$$\sigma\colon\ R \longrightarrow R$$

ein K-Algebraautomorphismus. Zeige, dass die Menge der abgeschlossenen Fixpunkte der Spektrumsabbildung

$$\sigma^*\colon\ \operatorname{Spek}(R) \longrightarrow \operatorname{Spek}(R)$$

gleich der Menge der abgeschlossenen Punkte in $V(M)$ mit $M = \{f - f\sigma | \ f \in R\}$ ist.

Aufgabe 15.14. (4 Punkte)

Es sei K ein algebraisch abgeschlossener Körper. Wir betrachten die natürliche Operation der symmetrischen Gruppe S_3 auf $\operatorname{Spek}(K[X,Y,Z])$ zusammen mit der Quotientenabbildung

$$\operatorname{Spek}(K[X,Y,Z]) \longrightarrow \operatorname{Spek}(K[E_1,E_2,E_3])\,.$$

Man gebe für jede mögliche Anzahl $n \in \{1,\ldots,6\}$ einen abgeschlossenen Punkt $P \in \operatorname{Spek}(K[E_1,E_2,E_3])$ an, derart, dass die Faser über P aus genau n Punkten besteht.

16. Vorlesung - Tensorprodukt I

In dieser Vorlesung führen wir eine wichtige Konstruktion für Moduln ein, das sogenannte *Tensorprodukt*. Die Eigenschaften des konstruierten Objektes sind dabei wichtiger als die Konstruktion selbst.

Das Tensorprodukt von Moduln

Definition 16.1. Es sei R ein kommutativer Ring und seien $V_1, \ldots, V_n, W$ R-Moduln. Eine Abbildung

$$\psi\colon\ V_1 \times \cdots \times V_n \longrightarrow W$$

heißt *R-multilinear*, wenn für jedes $i \in \{1, \ldots, n\}$ und jedes $(n-1)$-Tupel $(v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_n)$ (mit $v_j \in V_j$) die induzierte Abbildung

$$V_i \longrightarrow W,\ u \longmapsto \psi\left(v_1, \ldots, v_{i-1}, u, v_{i+1}, \ldots, v_n\right),$$

R-linear ist.

Bei $n = 2$ spricht man von *bilinear*.

Definition 16.2. Es sei R ein kommutativer Ring und $V_1, \ldots, V_n, W$ seien R-Moduln. Es sei F der von sämtlichen Symbolen $v_1 \otimes v_2 \otimes \cdots \otimes v_n$ (mit $v_i \in V_i$) erzeugte freie R-Modul. Es sei $U \subseteq F$ der von allen Elementen der Form

(1) $r\left(v_1 \otimes \cdots \otimes v_{i-1} \otimes v_i \otimes v_{i+1} \otimes \cdots \otimes v_n\right) - v_1 \otimes \cdots \otimes v_{i-1} \otimes rv_i \otimes v_{i+1} \otimes \cdots \otimes v_n$,

(2) $v_1 \otimes \cdots \otimes v_{i-1} \otimes (u+w) \otimes v_{i+1} \otimes \cdots \otimes v_n - v_1 \otimes \cdots \otimes v_{i-1} \otimes u \otimes v_{i+1} \otimes \cdots \otimes v_n - v_1 \otimes \cdots \otimes v_{i-1} \otimes w \otimes v_{i+1} \otimes \cdots \otimes v_n$,

erzeugte R-Untermodul. Dann nennt man den Restklassenmodul F/U das *Tensorprodukt* der V_i, $i \in \{1, \ldots, n\}$. Es wird mit

$$V_1 \otimes_R V_2 \otimes_R \cdots \otimes_R V_n$$

bezeichnet.

Die Bilder von $(v_1, \ldots, v_n)$ in $V_1 \otimes_R V_2 \otimes_R \cdots \otimes_R V_n$ bezeichnet man wieder mit $v_1 \otimes \cdots \otimes v_n$. Jedes Element aus $V_1 \otimes_R \cdots \otimes_R V_n$ besitzt eine (nicht eindeutige) Darstellung als

$$a_1 v_{1,1} \otimes \cdots \otimes v_{1,n} + \ldots + a_m v_{m,1} \otimes \cdots \otimes v_{m,n}$$

(mit $a_i \in R$ und $v_{i,j} \in V_j$). Insbesondere bilden die (*zerlegbaren Tensoren*) $v_1 \otimes \cdots \otimes v_n$ ein R-Modulerzeugendensystem des Tensorprodukts. Die definierenden Erzeuger des Untermoduls werden zu Gleichungen im Tensorprodukt, sie drücken die Multilinearität aus. Insbesondere gilt

$$v_1 \otimes \cdots \otimes v_{i-1} \otimes rv_i \otimes v_{i+1} \otimes \cdots \otimes v_n \ = \ v_1 \otimes \cdots \otimes v_{j-1} \otimes rv_j \otimes v_{j+1} \otimes \cdots \otimes v_n$$

für beliebige i, j.

Wichtiger als die Konstruktion des Tensorprodukts ist die folgende *universelle Eigenschaft*.

Lemma 16.3. *Es sei R ein kommutativer Ring und $V_1, \ldots, V_n$ seien R-Moduln.*

(1) *Die Abbildung*

$$\pi\colon V_1 \times \cdots \times V_n \longrightarrow V_1 \otimes_R \cdots \otimes_R V_n,\ (v_1, \ldots, v_n) \longmapsto v_1 \otimes \cdots \otimes v_n,$$

ist R-multilinear.

(2) *Es sei W ein weiterer R-Modul und*

$$\psi\colon V_1 \times \cdots \times V_n \longrightarrow W$$

eine multilineare Abbildung. Dann gibt es eine eindeutig bestimmte R-lineare Abbildung

$$\bar{\psi}\colon V_1 \otimes_R \cdots \otimes_R V_n \longrightarrow W$$

mit $\psi = \bar{\psi} \circ \pi$.

Beweis. (1) folgt unmittelbar aus der Definition des Tensorprodukts. (2). Da die $v_1 \otimes \cdots \otimes v_n$ ein R-Modulerzeugendensystem von $V_1 \otimes_R \cdots \otimes_R V_n$ sind und

$$\bar{\psi}(v_1 \otimes \cdots \otimes v_n) = \psi(v_1, \ldots, v_n)$$

gelten muss, kann es maximal eine solche lineare Abbildung geben. Zur Existenz betrachten wir den freien Modul F aus der Konstruktion des Tensorprodukts. Die Symbole $v_1 \otimes \cdots \otimes v_n$ bilden eine Basis von F, daher legt die Vorschrift $\varphi\,(v_1 \otimes \cdots \otimes v_n) := \psi(v_1 \otimes \cdots \otimes v_n)$ eine lineare Abbildung

$$F \longrightarrow W$$

fest. Wegen der Multilinearität von ψ wird der Untermodul U auf 0 abgebildet. Daher induziert diese Abbildung nach dem Faktorisierungssatz einen R-Modulhomomorphismus

$$F/U \cong V_1 \otimes_R \cdots \otimes_R V_n \longrightarrow W.$$

□

Das Tensorprodukt ist durch diese universelle Eigenschaft bis auf (eindeutige) Isomorphie festgelegt. Wenn es also einen R-Modul T zusammen mit einer multilinearen Abbildung $V_1 \times \cdots \times V_n \to T$ derart gibt, dass jede multilineare Abbildung in einen R-Modul W eindeutig über T mit einer linearer Abbildung von T nach W faktorisiert, so gibt es einen eindeutig bestimmten Isomorphismus zwischen T und dem Tensorprodukt $V_1 \otimes_R \cdots \otimes_R V_n$. Daher ist diese universelle Eigenschaft wichtiger als die oben durchgeführte Konstruktion des Tensorprodukts.

Proposition 16.4. *Es sei R ein kommutativer Ring und U, V, W seien R-Moduln. Dann gelten folgende Aussagen.*

(1) *Es ist*

$$U \otimes_R V \cong V \otimes_R U.$$

(2) *Es ist*

$$U \otimes_R (V \otimes_R W) \cong (U \otimes_R V) \otimes_R W.$$

(3) *Es ist*

$$U \otimes_R (V \oplus W) \cong (U \otimes_R V) \oplus (U \otimes_R W).$$

Beweis. Siehe Aufgabe 16.2. □

Proposition 16.5. *Es sei R ein kommutativer Ring und seien U, V, W, M R-Moduln. Dann gelten folgende Aussagen.*

(1) *Zu einem R-Modulhomomorphismus $\varphi\colon U \to V$ gibt es einen natürlichen R-Modulhomomorphismus $\varphi \otimes_R \mathrm{Id}_M\colon U \otimes_R M \to V \otimes_R M$.*
(2) *Zu einer exakten Sequenz*

$$U \longrightarrow V \longrightarrow W \longrightarrow 0$$

von R-Moduln ist auch

$$U \otimes_R M \longrightarrow V \otimes_R M \longrightarrow W \otimes_R M \longrightarrow 0$$

exakt.

Beweis. (1). Die Abbildung

$$U \times M \longrightarrow V \otimes_R M,\ (u, m) \longmapsto \varphi(u) \otimes m,$$

ist R-bilinear und induziert daher einen R-Modulhomomorphismus

$$U \otimes_R M \longrightarrow V \otimes_R M.$$

(2). Die Surjektivität der Abbildung

$$V \otimes_R M \longrightarrow W \otimes_R M$$

ist klar, da die $w \otimes m$ ein R-Modulerzeugendensystem von $W \otimes_R N$ bilden und diese im Bild der Abbildung liegen. Für die Exaktheit an der anderen Stelle müssen wir die Isomorphie

$$V \otimes_R M/\operatorname{bild}(U \otimes_R M) \cong W \otimes_R M$$

nachweisen. Dazu beweisen wir für diesen Restklassenmodul, dass er die universelle Eigenschaft des Tensorprodukts erfüllt. Es sei also

$$W \times M \longrightarrow N$$

eine R-multilineare Abbildung in einen R-Modul N. Somit liegt auch eine eindeutige multilineare Abbildung

$$\psi\colon V \times M \longrightarrow N$$

und damit eine R-lineare Abbildung

$$\tilde{\psi}\colon V \otimes_R M \longrightarrow N$$

vor. Wegen

$$\psi(\operatorname{bild} U \times M) = 0$$

ist

$$\tilde{\psi}(\operatorname{bild} U \otimes_R M) = 0$$

und daher gibt es eine eindeutige Faktorisierung

$$V \otimes_R M/\operatorname{bild}\,(U \otimes_R M) \longrightarrow N.$$

□

Ringwechsel

Wir betrachten jetzt den Fall des Tensorproduktes, wenn über R ein R-Modul M und eine kommutative R-Algebra R' vorliegt.

Definition 16.6. Zu einem R-Modul M und einem Ringhomomorphismus

$$R \longrightarrow R'$$

zwischen kommutativen Ringen nennt man $R' \otimes_R M$ den *durch Ringwechsel gewonnenen R'-Modul*.

Beispiel 16.7. Es sei V ein reeller Vektorraum. Die Tensorierung mit der $\mathbb{R}$-Algebra $\mathbb{C}$, also

$$V_{\mathbb{C}} := \mathbb{C} \otimes_{\mathbb{R}} V,$$

nennt man die *Komplexifizierung* von V. Wenn V die Dimension n besitzt, so besitzt $V_{\mathbb{C}}$ als komplexer Vektorraum ebenfalls die Dimension n. Wenn man $V_{\mathbb{C}}$ als reellen Vektorraum betrachtet, so besitzt er die reelle Dimension $2n$.

Proposition 16.8. *Es sei R ein kommutativer Ring, M ein R-Modul und $R \to R'$ ein Ringhomomorphismus. Dann gelten folgende Aussagen.*

(1) *Das Tensorprodukt $R' \otimes_R M$ ist ein R'-Modul.*
(2) *Es gibt einen kanonischen R-Modulhomomorphismus*

$$M \longrightarrow R' \otimes_R M,\ v \longmapsto 1 \otimes v.$$

Bei $R = R'$ ist dies ein Isomorphismus.
(3) *Zu einem R-Modulhomomorphismus $\varphi\colon M \to N$ ist die induzierte Abbildung*

$$\mathrm{Id}_{R'} \otimes \varphi\colon\ R' \otimes_R M \longrightarrow R' \otimes_R N$$

ein R'-Modulhomomorphismus.
(4) *Zu $M = R^n$ ist*

$$R' \otimes_R R^n \cong (R')^n.$$

(5) *Zu einem weiteren Ringhomomorphismus $R' \to R''$ ist*

$$R'' \otimes_R M \cong R'' \otimes_{R'} (R' \otimes_R M)$$

(eine Isomorphie von R''-Moduln).

Beweis. (1). Die Multiplikation

$$R' \times R' \longrightarrow R', (r,s) \longmapsto rs,$$

ist R'-bilinear und führt nach Lemma 16.3 zu einer R'-linearen Abbildung

$$R' \otimes_R R' \longrightarrow R'.$$

Dies induziert nach Proposition 16.4 (2) und nach Proposition 16.5 einen R-Modulhomomorphismus

$$R' \otimes_R (R' \otimes_R M) \cong (R' \otimes_R R') \otimes_R M \longrightarrow R' \otimes_R M.$$

Dies ergibt eine wohldefinierte Skalarmultiplikation

$$R' \times (R' \otimes_R M) \longrightarrow (R' \otimes_R M),$$

die explizit durch[7]

$$s \cdot \left(\sum_{j=1}^{n} r_j \otimes m_j \right) = \sum_{j=1}^{n} (sr_j) \otimes m_j$$

gegeben ist. Aus dieser Beschreibung folgen direkt die Eigenschaften einer Skalarmultiplikation. (2). Die R-Homomorphie folgt direkt aus der Bilinearität des Tensorprodukts. Bei $R' = R$ ist die Abbildung surjektiv. Die Skalarmultiplikation $R \times M \to M$ induziert eine R-lineare Abbildung

$$R \otimes_R M \longrightarrow M.$$

Die Verknüpfung der kanonischen Abbildung $M \to R \otimes_R M$ mit dieser Abbildung ist die Identität auf M, so dass die erste Abbildung auch injektiv ist. (3) folgt aus der expliziten Beschreibung in (1). (4) folgt aus Proposition 16.4 (3).(5). Nach Teil (2) haben wir einerseits eine R-lineare Abbildung $M \to R' \otimes_R M$. Dies führt zu einer R-multilinearen Abbildung

$$R'' \times M \longrightarrow R'' \times (R' \otimes_R M) \longrightarrow R'' \otimes_{R'} (R' \otimes_R M),$$

die eine R-lineare Abbildung

$$R'' \otimes_R M \longrightarrow R'' \otimes_{R'} (R' \otimes_R M)$$

induziert. Andererseits haben wir eine R'-lineare Abbildung

$$R' \otimes_R M \longrightarrow R'' \otimes_R M.$$

Rechts steht ein R''-Modul, daher kann man die Skalarmultiplikation als eine R'-multilineare Abbildung

$$R'' \times (R' \otimes_R M) \longrightarrow R'' \otimes_R M$$

auffassen, die ihrerseits zu einer R'-linearen Abbildung

$$R'' \otimes_{R'} (R' \otimes_R M) \longrightarrow R'' \otimes_R M$$

[7]Wenn man die Skalarmultiplikation direkt über diese Formel definieren möchte hat man das Problem der Wohldefiniertheit.

führt. Diese beiden Abbildungen sind invers zueinander, was man auf den zerlegbaren Tensoren überprüfen kann. Daran sieht man auch, dass sich die R''-Multiplikationen entsprechen. □

Proposition 16.9. *Es sei R ein kommutativer Ring und M ein R-Modul. Dann gelten folgende Aussagen.*

(1) *Zu einem multiplikativen System $S \subseteq R$ ist $M_S \cong R_S \otimes_R M$.*
(2) *Zu einem Ideal $I \subseteq R$ ist $M/IM \cong R/I \otimes_R M$.*

Beweis. Siehe Aufgabe 16.4. □

Beispiel 16.10. Zu einem Integritätsbereich R mit Quotientenkörper $Q(R)$ und einem R-Modul M erhält man im Tensorprodukt $Q(R) \otimes_R M$ einen Modul über dem Quotientenkörper $Q(R)$, also einen Vektorraum. Dieser Vektorraum trägt häufig schon wesentliche Informationen über den Modul. Seine Dimension nennt man auch den *Rang* des Moduls.

Beispiel 16.11. Zu jeder kommutativen Gruppe H und jedem kommutativen Ring R enthält man im Tensorprodukt $R \otimes_{\mathbb{Z}} H$ einen R-Modul. Wenn H endlich erzeugt und die Zerlegung (vergleiche den Hauptsatz über endlich erzeugte kommutative Gruppen)

$$H \cong \mathbb{Z}^r \times \mathbb{Z}/(n_1) \times \cdots \times \mathbb{Z}/(n_s)$$

vorliegt, so ist der tensorierte Modul die direkte Summe aus R^r und den

$$R \otimes_{\mathbb{Z}} \mathbb{Z}/(n_j) \cong R/(n_j R),$$

wobei deren Gestalt von der Charakteristik des Ringes abhängt.

Beispiel 16.12. Es sei G eine Gruppe, die auf einem kommutativen Ring R als Gruppe von Ringautomorphismen operiere, und es sei R^G der Invariantenring. Dann gehört zu jedem R^G-Modul M das Tensorprodukt $R \otimes_{R^G} M$. Auf diesem R-Modul operiert die Gruppe G in natürlicher und mit der Operation auf R verträglichen Weise, siehe Aufgabe 16.10.

16. Arbeitsblatt

Aufwärmaufgaben

Aufgabe 16.1. Es sei R ein kommutativer Ring und M ein R-Modul. Zeige, dass die Skalarmultiplikation

$$R \times M \longrightarrow M,\ (r, m) \longmapsto rm,$$

R-bilinear ist.

Aufgabe 16.2. Es sei R ein kommutativer Ring und U, V, W seien R-Moduln. Zeige die folgenden Aussagen.

(1) Es ist
$$U \otimes_R V \cong V \otimes_R U.$$
(2) Es ist
$$U \otimes_R (V \otimes_R W) \cong (U \otimes_R V) \otimes_R W.$$
(3) Es ist
$$U \otimes_R (V \oplus W) \cong (U \otimes_R V) \oplus (U \otimes_R W).$$

Aufgabe 16.3. Es sei R ein kommutativer Ring. Zeige die R-Modulisomorphie
$$R^n \otimes_R R^m \cong R^{nm}.$$

Aufgabe 16.4. Es sei R ein kommutativer Ring und M ein R-Modul. Zeige folgende Aussagen.

(1) Zu einem multiplikativen System $S \subseteq R$ ist $M_S \cong R_S \otimes_R M$.
(2) Zu einem Ideal $I \subseteq R$ ist $M/IM \cong R/I \otimes_R M$.

Aufgabe 16.5. Es seien R und S kommutative Ringe und $R \subseteq S$ sei ein direkter Summand. Zeige, dass für jeden R-Modul M die natürliche Abbildung
$$M \longrightarrow S \otimes_R M$$
injektiv ist.

Es sei R ein kommutativer Ring. Ein R-Modul M heißt *flach*, wenn die Tensorierung mit M die Exaktheit von beliebigen Sequenzen erhält.

Aufgabe 16.6. Es sei R ein kommutativer Ring. Zeige, dass der R-Modul R^n flach ist.

Aufgabe 16.7. Man gebe ein Beispiel eines nicht flachen Moduls über einem kommutativen Ring.

Aufgabe 16.8. Es sei H eine endlich erzeugte kommutative Gruppe und
$$H \cong \mathbb{Z}^r \times \mathbb{Z}/(n_1) \times \cdots \times \mathbb{Z}/(n_s)$$
eine direkte Zerlegung (mit $n_j \in \mathbb{N}_+$). Zeige mit Hilfe des Tensorproduktes, dass die Zahl r in jeder direkten Zerlegung von H gleich ist.

Aufgabe 16.9. Es sei K ein Körper, R eine kommutative K-Algebra und G eine Gruppe, die als Gruppe von K-Algebraautomorphismen auf R operiere. Ferner liege eine lineare Operation von G auf einem endlichdimensionalen K-Vektorraum V vor. Zeige, dass auf dem R-Modul $R \otimes_K V$ eine verträgliche Operation von G als Gruppe von R-Modulautomorphismen vorliegt.

Aufgabe 16.10. Es sei R ein kommutativer Ring, auf dem eine Gruppe G als Gruppe von Ringautomorphismen operiere mit dem Invariantenring R^G. Es sei M ein R^G-Modul und $R \otimes_{R^G} M$ der durch Ringwechsel gewonnene R-Modul. Zeige, dass es eine verträgliche Operation von G auf $R \otimes_{R^G} M$ als Gruppe von R-Modulautomorphismen gibt, und dass es eine natürliche Abbildung

$$M \longrightarrow (R \otimes_{R^G} M)^G$$

gibt. Zeige, dass unter der Bedingung, dass R^G ein direkter Summand von R ist, diese Abbildung injektiv ist, und dass dies ohne diese Voraussetzung nicht gelten muss.

Aufgaben zum Abgeben

Aufgabe 16.11. (3 Punkte)

Berechne das Tensorprodukt

$$\left(\mathbb{Z}^3 \oplus (\mathbb{Z}/(2))^2 \oplus \mathbb{Z}/(3)\right) \otimes_{\mathbb{Z}} \left(\mathbb{Z}^2 \oplus \mathbb{Z}/(2) \oplus \mathbb{Z}/(4)\right) .$$

Aufgabe 16.12. (3 Punkte)

Es sei R ein kommutativer Ring und $S \subseteq R$ ein multiplikatives System. Zeige, dass der R-Modul R_S flach ist.

17. Vorlesung - Tensorprodukt II

Tensorprodukt von Ringen

Wir betrachten jetzt die Situation, in der zwei kommutative R-Algebren vorliegen.

Lemma 17.1. *Es sei R ein kommutativer Ring und A, B seien kommutative R-Algebren. Dann ist das Tensorprodukt*

$$A \otimes_R B$$

eine kommutative R-Algebra und es gibt R-Algebrahomomorphismen

$$A \longrightarrow A \otimes_R B,\ a \longmapsto a \otimes 1,$$

und

$$B \longrightarrow A \otimes_R B,\, b \longmapsto 1 \otimes b.$$

Beweis. Die Multiplikationen auf A bzw. auf B führen zu R-linearen Abbildungen $\mu_A\colon\ A \otimes_R A \to A$ und $\mu_B\colon\ B \otimes_R B \to B$. Dies ergibt eine R-bilineare Abbildung

$$(A \otimes_R A) \times (B \otimes_R B) \longrightarrow A \otimes_R B$$

und damit zu einer R-linearen Abbildung

$$\mu\colon\ (A \otimes_R A) \otimes_R (B \otimes_R B) \longrightarrow A \otimes_R B.$$

Aufgrund der Kommutativität des Tensorprodukts können wir dies als eine R-lineare Abbildung

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

auffassen, wodurch eine Multiplikation auf $A \otimes_R B$ definiert wird. Diese Multiplikation wird auf den zerlegbaren Tensoren explizit durch

$$(a_1 \otimes b_1) \cdot (a_2 \otimes b_2) \ = \ a_1a_2 \otimes b_1b_2$$

und allgemein durch

$$\left(\sum_{i=1}^{m} a_i \otimes b_i\right) \cdot \left(\sum_{j=1}^{n} c_j \otimes d_j\right) \ = \ \sum_{i,j} a_ic_j \otimes b_ib_j$$

gegeben. Die bisherige Überlegung sichert, dass dies wohldefiniert ist. Der Nachweis, dass durch diese Multiplikation das Tensorprodukt zu einem kommutativen Ring wird, erfolgt über diese explizite Beschreibung, wobei man sich auf die zerlegbaren Elementen beschränken kann. Dass Ringhomomorphismen vorliegen ergibt sich ebenfalls aus der expliziten Beschreibung. □

Beispiel 17.2. Zu einem kommutativen Ring R und den Polynomringen $A = R[X_1, \ldots, X_m]$ und $B = R[Y_1, \ldots, Y_n]$ ist

$$A \otimes_R B \ = \ R[X_1, \ldots, X_m, Y_1, \ldots, Y_n].$$

Die Vorgabe $X_i \mapsto X_i \otimes 1$ und $Y_j \mapsto 1 \otimes Y_j$ definiert den Einsetzungshomomorphismus

$$R[X_1, \ldots, X_m, Y_1, \ldots, Y_n] \longrightarrow A \otimes_R B.$$

Die Zuordnung

$$A \times B \longrightarrow R[X_1, \ldots, X_m, Y_1, \ldots, Y_n],\, (a, b) \longmapsto a \cdot b,$$

ist R-bilinear und definiert nach Lemma 16.3 (2) einen R-Modulhomomorphismus

$$A \otimes_R B \longrightarrow R[X_1, \ldots, X_m, Y_1, \ldots, Y_n].$$

Beide Abbildungen sind invers zueinander.

Beispiel 17.3. Zu einem kommutativen Ring R und endlich erzeugten R-Algebren $A = R[X_1, \ldots, X_m]/\mathfrak{a}$ und $B = R[Y_1, \ldots, Y_n]/\mathfrak{b}$ ist

$$A \otimes_R B \,=\, R[X_1, \ldots, X_m, Y_1, \ldots, Y_n]/(\mathfrak{a} + \mathfrak{b}).$$

Dies wird ähnlich wie die Isomorphie in Beispiel 17.2 begründet.

Beispiel 17.4. Es sei $\varphi\colon\, R \to S$ ein Ringhomomorphismus zwischen kommutativen Ringen und

$$\varphi^*\colon\, \operatorname{Spek}(S) \longrightarrow \operatorname{Spek}(R)$$

die zugehörige Spektrumsabbildung. Zu einem Primideal $\mathfrak{p} \in \operatorname{Spek}(R)$ ist die Faser zu φ^* über $\mathfrak{p}$ gleich $\operatorname{Spek}(\kappa(\mathfrak{p}) \otimes_R S)$. Dies folgt aus

$$\kappa(\mathfrak{p}) \otimes_R S \,=\, R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}} \otimes_R S \,\cong\, (S/\mathfrak{p})_{\varphi(R\setminus\mathfrak{p})}$$

(nach Proposition 16.9) und der Beschreibung der Faser in Lemma 14.3.

Satz 17.5. *Es sei R ein kommutativer Ring und A, B, S seien kommutative R-Algebren. Dann ist*

$$\operatorname{Hom}_R^{\mathrm{alg}}(A \otimes_R B, S) \,=\, \operatorname{Hom}_R^{\mathrm{alg}}(A, S) \times \operatorname{Hom}_R^{\mathrm{alg}}(B, S)\,.$$

Beweis. Über die natürlichen R-Algebrahomomorphismen (siehe Lemma 17.1)

$$A \longrightarrow A \otimes_R B,\, a \longmapsto a \otimes 1,$$

und

$$B \longrightarrow A \otimes_R B,\, b \longmapsto 1 \otimes b,$$

erhält man eine Abbildung von links nach rechts. Da die $a \otimes 1$ und $1 \otimes b$ ein R-Algebraerzeugendensystem von $A \otimes_R B$ bilden, ist darauf ein R-Algebrahomomorphismus nach S festgelegt. Es kann also zu

$$(\varphi, \psi) \in \operatorname{Hom}_R^{\mathrm{alg}}(A, S) \times \operatorname{Hom}_R^{\mathrm{alg}}(B, S)$$

maximal einen Homomorphismus links geben, der darauf abbildet. Die Abbildung ist also injektiv. Zum Nachweis der Surjektivität sei (φ, ψ) gegeben. Wir betrachten die Abbildung

$$A \times B \longrightarrow S,\, (a, b) \longmapsto \varphi(a)\psi(b).$$

Diese Abbildung ist offenbar R-bilinear, daher gibt es dazu nach Lemma 16.3 einen R-Modulhomomorphismus

$$\theta\colon\, A \otimes_R B \longrightarrow S.$$

Dieser ist wegen

$$\begin{aligned}
\theta(a_1 \otimes b_1 \cdot a_2 \otimes b_2) &= \theta(a_1a_2 \otimes b_1b_2) \\
&= \varphi(a_1a_2) \cdot \psi(b_1b_2) \\
&= \varphi(a_1)\varphi(a_2)\psi(b_1)\psi(b_2) \\
&= \theta(a_1 \otimes b_1) \cdot \theta(a_2 \otimes b_2)
\end{aligned}$$

auch mit der Multiplikation verträglich. □

Bei $Z = \operatorname{Spek}(R)$, $X = \operatorname{Spek}(A)$ und $Y = \operatorname{Spek}(B)$ schreibt man auch

$$X \times_Z Y \;=\; \operatorname{Spek}(A \otimes_R B)$$

(manchmal auch $X \times_R Y$) und nennt dies das *Produkt der affinen Schemata* X und Y (über Z). Der obige Satz übersetzt sich zur folgenden universellen Eigenschaft dieses Produkts: Zu einem affinen Schemamorphismus (also einer Spektrumsabbildung)

$$\psi\colon\; T = \operatorname{Spek}(C) \longrightarrow Z = \operatorname{Spek}(R)$$

und zwei Morphismen $\varphi_1\colon\; T \to X$ und $\varphi_2\colon\; T \to Y$ über ψ gibt es einen eindeutigen Morphismus

$$\varphi\colon\; T \longrightarrow X \times_Z Y,$$

der mit allen vorgegebenen Morphismen kommutiert. Wenn $Z = \operatorname{Spek}(K)$ das Spektrum eines Körpers ist, so bedeutet dies für die K-wertigen Punkte insbesondere

$$(X \times_Z Y)(K) \;=\; X(K) \times Y(K).$$

Hopf-Algebren und affine Gruppenschemata

Wir haben zu einer Operation einer Gruppe G auf einem kommutativen Ring R eine geometrische Interpretation gefunden, nämlich die Operation der Gruppe auf dem Spektrum von R. Der Ring bildet zusammen mit seinem Spektrum eine algebraisch-geometrische Einheit, und die Gruppenwirkung hat algebraische und geometrische Eigenschaften, die eng miteinander verflochten sind. Die Gruppenoperation können wir als einen Gruppenhomomorphismus in die Automorphismengruppe des Ringes oder des affinen Schemas auffassen. Wir haben aber bisher noch keine Sprache dafür, ob die Operation als Ganzes algebraisch-geometrisch ist, und wir haben noch nicht geklärt, ob wir die operierende Gruppe eher als ein algebraisches oder als ein geometrisches Objekt ansehen wollen.

Zum ersten Problemkreis betrachten wir einerseits die multiplikative Gruppe $(K^\times, 1, \cdot)$ und andererseits die additive Gruppe $(K, 0, +)$ zu einem Körper K. Die typischen Operationen dieser beiden Gruppen haben ziemlich verschiedene Eigenschaften. Die multiplikativen Operationen sind „diagonalisierbar“ und eng mit den Graduierungen (siehe Satz 7.10) verbunden, die Invariantenringe sind daher recht einfach zu berechnen und sind insbesondere direkte Summanden. Letzteres muss für die additive Gruppe nicht gelten, wie Beispiel 6.9 (vergleiche auch Beispiel 15.9) zeigt. Dieser Unterschied ist aber bisher lediglich eine Beobachtung, da wir nur einige Beispiele von Operationen dieser Gruppen betrachtet, aber noch nicht fixiert haben, auf welche Art diese Gruppen operieren sollen.

Beispiel 17.6. Die Exponentialfunktion ist bekanntlich ein Gruppenisomorphismus

$$(\mathbb{R}, 0, +) \longrightarrow (\mathbb{R}_+, 1, \cdot) \subset \mathbb{R}^\times,\ t \longmapsto e^t,$$

mit dem natürlichen Logarithmus als Umkehrfunktion. Daher kann man jede Gruppenoperation der additiven Gruppe $\mathbb{R}$ auf einer beliebigen Menge auch als eine Operation der positiven multiplikativen Gruppe $\mathbb{R}_+$ ansehen und umgekehrt. Sämtliche operationstheoretischen Konzepte wie Bahn, Isotropiegruppe, Invariantenring stimmen dabei überein. Beispielsweise kann man die skalare Multiplikation von $\mathbb{R}^\times$ auf dem $\mathbb{R}^n$ als die Operation

$$(\mathbb{R}, 0, +) \times \mathbb{R}^n \longrightarrow \mathbb{R}^n,\ (t, x_1, \ldots, x_n) \longmapsto (e^t x_1, \ldots, e^t x_n),$$

auffassen. Diese Operation kann man nur unter Verwendung einer transzendenten Funktion hinschreiben. Wenn man nur „algebraische Operationen“ zulassen möchte, so sind die multiplikative und die additive Gruppe nicht isomorph, und sie besitzen sehr unterschiedliche Operationen.

Die Gruppenaxiome kann man durch die folgenden kommutativen Diagramme ausdrücken. Dabei sei G die Gruppe, μ die Multiplikation, e das neutrale Element und inv die Inversenabbildung.

$$\begin{array}{ccc} G \times G \times G & \stackrel{\mu \times \mathrm{Id}_G}{\longrightarrow} & G \times G \\ {\scriptstyle \mathrm{Id}_G \times \mu}\downarrow & & \downarrow{\scriptstyle \mu} \\ G \times G & \stackrel{\mu}{\longrightarrow} & G \end{array}$$

$$\begin{array}{ccc} G & \stackrel{\mathrm{Id} \times e}{\longrightarrow} & G \times G \\ & {\scriptstyle \mathrm{Id}_G}\searrow & \downarrow{\scriptstyle \mu} \\ & & G \end{array}$$

$$\begin{array}{ccc} G & \stackrel{\mathrm{inv} \times \mathrm{Id}_G}{\longrightarrow} & G \times G \\ \downarrow & & \downarrow{\scriptstyle \mu} \\ \{e\} & \longrightarrow & G \end{array}$$

Die duale Formulierung dieser Diagramme führt zum Begriff der *Hopf-Algebra*.

Definition 17.7. Es sei K ein kommutativer Ring.[8] Eine kommutative K-Algebra H heißt *Hopf-Algebra*, wenn es fixierte K-Algebrahomomorphismen (genannt *Komultiplikation*, *Koeinheit* und *Koinverses*)

$$\Delta\colon\ H \longrightarrow H \otimes_K H,$$

$$\epsilon\colon\ H \longrightarrow K$$

[8]Wir schreiben hier K für den kommutativen Grundring; die Schlagkraft des Konzeptes zeigt sich bereits vollständig im Fall, dass K ein Körper ist, so dass man sich unter K gerne einen Körper vorstellen kann.

und

$$S\colon\ H \longrightarrow H$$

gibt, derart, dass die Diagramme

$$\begin{array}{ccc} H & \stackrel{\Delta}{\longrightarrow} & H \otimes_K H \\ \Delta\downarrow & & \downarrow \mathrm{Id}_H \otimes \Delta \\ H \otimes_K H & \stackrel{\Delta\otimes \mathrm{Id}_H}{\longrightarrow} & H \otimes_K H \otimes_K H\ , \end{array}$$

$$\begin{array}{ccc} H & \stackrel{\Delta}{\longrightarrow} & H \otimes_K H \\ & \cong\searrow & \downarrow \epsilon \otimes \mathrm{Id}_H \\ & & K \otimes_K H \end{array}$$

und

$$\begin{array}{ccc} H & \stackrel{\Delta}{\longrightarrow} & H \otimes_K H \\ \epsilon\downarrow & & \downarrow \mathrm{Id}_H \cdot S \\ K & \longrightarrow & H \end{array}$$

kommutieren.

Beispiel 17.8. Es sei $(G, 1, \cdot)$ eine endliche Gruppe und K ein kommutativer Ring. Wir setzen

$$H\ :=\ \mathrm{Abb}\ (G, K)$$

mit der Addition und Multiplikation von Abbildungen, die unabhängig von G sind. Wir definieren auf H eine Hopf-Algebra-Struktur unter Verwendung der Gruppenstruktur. Die Gruppenmultiplikation

$$\mu\colon\ G \times G \longrightarrow G$$

führt zur Abbildung

$$\mathrm{Abb}\ (G, K) \longrightarrow \mathrm{Abb}\ (G, K) \otimes \mathrm{Abb}\ (G, K) \cong \mathrm{Abb}\ (G \times G, K)\,,\ f \longmapsto f \circ \mu,$$

wodurch wir die Komultiplikation

$$\Delta\colon\ H \longrightarrow H \otimes_K H$$

festlegen. Das Basiselement e_σ zu $\sigma \in G$ wird dabei auf

$$\sum_{\tau\cdot\rho=\sigma} e_\tau \otimes e_\rho\ =\ \sum_\tau e_\tau \otimes e_{\tau^{-1}\cdot\sigma}$$

abgebildet. Das neutrale Element $1 \in G$ induziert die Auswertungsabbildung

$$\epsilon\colon\ H = \mathrm{Abb}\ (G, K) \longrightarrow K,\ f \longmapsto f(1),$$

und die Inversenbildung

$$\mathrm{inv}\colon\ G \longrightarrow G,\ \sigma \longmapsto \sigma^{-1},$$

führt zu

$$S\colon\ \mathrm{Abb}\ (G, K) \longrightarrow \mathrm{Abb}\ (G, K)\,,\ f \longmapsto f \circ \mathrm{inv},$$

wobei das Basiselement e_σ auf $e_{\sigma^{-1}}$ abgebildet wird. Die Abbildungen Δ, ϵ, S sind offenbar K-Algebrahomomorphismen. Die Gruppenaxiome kann man durch die Kommutativität geeigneter Diagramme ausdrücken. Wendet man auf diese den Funktor Abb $(-, K)$ in Zusammenhang mit geeigneten Identifizierungen an, so erhält man die Kommutativität der Diagramme in der Definition einer Hopf-Algebra.

Beispiel 17.9. Es sei K ein kommutativer Ring. Auf dem Polynomring $K[X]$ kann man folgendermaßen eine Hopf-Struktur erklären. Die Komultiplikation wird durch

$$\Delta\colon\ K[X] \longrightarrow K[X] \otimes_K K[X] \cong K[X,Y],\ X \longmapsto X \otimes 1 + 1 \otimes X = X + Y,$$

erklärt. Die Koeinheit wird durch

$$K[X] \longrightarrow K,\ X \longmapsto 0,$$

festgelegt und das Koinverse ist durch

$$K[X] \longrightarrow K[X],\ X \longmapsto -X,$$

definiert. Nach Aufgabe 17.14 ist dies in der Tat eine Hopf-Algebra, die man die *Hopf-Algebra der additiven Gruppe* nennt.

Beispiel 17.10. Es sei K ein kommutativer Ring. Auf $K[X, X^{-1}] \cong K[X]_X$ kann man folgendermaßen eine Hopf-Struktur erklären. Die Komultiplikation wird durch

$$\begin{aligned}\Delta : K[X,X^{-1}] \longrightarrow K[X,X^{-1}] \otimes_K K[X,X^{-1}] \cong K[X,X^{-1},Y,Y^{-1}],\\ X \longmapsto X \otimes 1 \cdot 1 \otimes X = X \cdot Y,\end{aligned}$$

erklärt. Die Koeinheit wird durch

$$K[X] \longrightarrow K,\ X \longmapsto 1,$$

festgelegt und das Koinverse ist durch

$$K[X,X^{-1}] \longrightarrow K[X,X^{-1}],\ X \longmapsto X^{-1},$$

definiert. Nach Aufgabe 17.17 ist dies in der Tat eine Hopf-Algebra, die man die *Hopf-Algebra der multiplikativen Gruppe* nennt.

Beispiel 17.11. Es sei $(D, 0, +)$ eine kommutative Gruppe, K ein kommutativer Ring und $K[D]$ der zugehörige Gruppenring, also

$$K[D] = \bigoplus_{d \in D} KX^d.$$

Darauf lässt sich die Struktur einer Hopf-Algebra erklären, indem man die Komultiplikation als

$$\Delta\colon\ K[D] \longrightarrow K[D] \otimes_K K[D],\ X^d \longmapsto X^d \otimes X^d,$$

die Koeinheit als

$$\epsilon\colon\ K[D] \longrightarrow K,\ X^d \longmapsto X^0 = 1,$$

und das Koinverse als

$$S\colon\ K[D] \longrightarrow K[D],\ X^d \longmapsto X^{-d},$$

ansetzt. Diese K-Algebrahomomorphismen gehören zu den Gruppenhomomorphismen $D \to D \times D$, $d \mapsto (d,d)$, $D \to 0$ und $D \to D$, $d \mapsto -d$, im Sinne von Korollar 8.6.

Die Konstruktion in Beispiel 17.10 ist ein Spezialfall der Hopf-Algebrastruktur auf einem Gruppenring, nämlich für $D = \mathbb{Z}$.

17. Arbeitsblatt

Aufwärmaufgaben

Aufgabe 17.1. Es sei R ein kommutativer Ring und $\mathfrak{a}, \mathfrak{b} \subseteq R$ seien Ideale. Zeige die R-Algebraisomorphie

$$R/\mathfrak{a} \otimes_R R/\mathfrak{b} \ = \ R/\left(\mathfrak{a}+\mathfrak{b}\right).$$

Aufgabe 17.2. Es sei R ein kommutativer Ring und $S, T \subseteq R$ seien multiplikative Systeme. Zeige die R-Algebraisomorphie

$$R_S \otimes_R R_T \ = \ R_{S\cdot T}.$$

Aufgabe 17.3. Es sei $K \subseteq L$ eine Körpererweiterung. Zeige, dass $L \otimes_K L$ kein Körper sein muss.

Aufgabe 17.4. Es sei

$$\varphi\colon\ R \longrightarrow S$$

ein ganzer Ringhomomorphismus zwischen kommutativen Ringen und $R \to R'$ ein weiterer Ringhomomorphismus. Zeige, dass auch

$$\varphi'\colon\ R' \longrightarrow R' \otimes_R S,\ f \longmapsto f \otimes 1,$$

ganz ist.

Aufgabe 17.5. Es sei K ein Körper und $n \in \mathbb{N}_+$. Bestimme zur Spektrumsabbildung

$$\varphi^*\colon\ \operatorname{Spek}\left(K[X]\right) \longrightarrow \operatorname{Spek}\left(K[X]\right)$$

zum Ringhomomorphismus

$$\varphi\colon\ K[X] \longrightarrow K[X],\ X \longmapsto X^n,$$

die Fasern zu jedem Punkt $\mathfrak{p} \in \operatorname{Spek}\left(K[X]\right)$. Worin unterscheiden sich die Fasern, welche Eigenschaften sind für jede Faser gleich? Wie viele Isomorphietypen der Fasern gibt es bei K algebraisch abgeschlossen?

Aufgabe 17.6. Es sei K ein Körper und sei $K[X]$ der Polynomring über K und $L = K(X)$ sein Quotientenkörper. Bestimme die L-wertigen Punkte von $K[X] \otimes_K K[X]$. Welcher Punkt entspricht der (zweifach genommenen) natürlichen Inklusion $K[X] \subseteq K(X)$?

Aufgabe 17.7. Es sei R ein kommutativer Ring und es seien $A = \bigoplus_{d \in D} A_d$ und $B = \bigoplus_{e \in E} B_e$ kommutative graduierte R-Algebren, wobei D und E kommutative Gruppen seien. Zeige, dass $A \otimes_R B$ in natürlicher Weise eine $D \times E$-Graduierung trägt.

Aufgabe 17.8. Es sei R ein kommutativer Ring und es seien A und B kommutative R-Algebren. Es seien H und G Gruppen, wobei die Gruppe H auf A und die Gruppe G auf B jeweils als Gruppe von R-Algebrahomomorphismen operiere. Zeige, dass dann eine natürliche Operation der Produktgruppe $H \times G$ auf $A \otimes_R B$ vorliegt.

Aufgabe 17.9. Es sei G eine Gruppe, die auf einer kommutativen R-Algebra A als Gruppe von R-Algebrahomomorphismen operiere. Zeige, dass G in natürlicher Weise auch auf den Tensorprodukten $A \otimes_R A$, $A \otimes_R A \otimes_R A$, etc. operiert.

Man überlege sich auch, wo die vorstehende Konstruktion im Laufe der Vorlesung vorkam (ohne dass explizit das Tensorprodukt verwendet wurde).

Aufgabe 17.10. Es sei R ein kommutativer Ring und seien A, B kommutative R-Algebren. Es sei G eine Gruppe, die auf R, A, B als Gruppe von Ringautomorphismen operiere, wobei die Operationen mit den Strukturhomomorphismen verträglich seien.

(1) Zeige, dass G in natürlicher Weise auf $A \otimes_R B$ operiert.
(2) Zeige, dass es einen Ringhomomorphismus
$$A^G \otimes_{R^G} B^G \longrightarrow (A \otimes_R B)^G$$
gibt.
(3) Man gebe ein Beispiel, das zeigt, dass der Ringhomomorphismus aus (2) kein Isomorphismus sein muss.

Zu einem Körper K, zwei Mengen X, Y und Funktionen $f\colon X \to K$ und $g\colon Y \to K$ schreiben wir $f \cdot g$ für die Abbildung $X \times Y \to K$, $(x, y) \mapsto f(x)g(y)$.

Aufgabe 17.11. Es sei K ein Körper und seien X und Y endliche Mengen. Zeige, dass man jede Funktion

$$h\colon X \times Y \longrightarrow K$$

in der Form

$$h = \sum_{i=1}^{n} f_i \cdot g_i$$

mit Funktionen $f_i\colon X \to K$ und $g_i\colon Y \to K$ schreiben kann.

Aufgabe 17.12. Es sei K ein Körper. Zeige, dass man nicht jede Funktion

$$h\colon \mathbb{N} \times \mathbb{N} \longrightarrow K$$

in der Form

$$h = \sum_{i=1}^{n} f_i \cdot g_i$$

mit Funktionen $f_i\colon \mathbb{N} \to K$ und $g_i\colon \mathbb{N} \to K$ schreiben kann.

Aufgabe 17.13. Zeige, dass man nicht jede stetige Funktion

$$h\colon \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R}$$

in der Form

$$h = \sum_{i=1}^{n} f_i \cdot g_i$$

mit stetigen Funktionen $f_i, g_i\colon \mathbb{R} \to \mathbb{R}$ schreiben kann.

Aufgabe 17.14. Wo wird in Beispiel 17.8 die Endlichkeit der Gruppe verwendet?

Aufgabe 17.15. Es sei K ein kommutativer Ring. Zeige, dass auf dem Polynomring $K[X]$ durch

$$\Delta\colon K[X] \longrightarrow K[X] \otimes_K K[X] \cong K[X,Y],\ X \longmapsto X \otimes 1 + 1 \otimes X = X + Y,$$

durch

$$K[X] \longrightarrow K,\ X \longmapsto 0,$$

und durch

$$K[X] \longrightarrow K[X],\ X \longmapsto -X,$$

eine Hopf-Struktur erklärt wird.

Aufgaben zum Abgeben

Aufgabe 17.16. (3 Punkte)

Es seien M und N kommutative Monoide und R ein kommutativer Ring. Zeige die R-Algebraisomorphie

$$R[M \times N] \cong R[M] \otimes_R R[N].$$

Aufgabe 17.17. (8 Punkte)

Zeige, dass man die Funktion

$$h\colon \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R},\ (x,y) \longmapsto \sqrt{x^2+y^2},$$

nicht in der Form

$$h = \sum_{i=1}^{n} f_i \cdot g_i$$

mit stetigen Funktionen $f_i, g_i\colon \mathbb{R} \to \mathbb{R}$ schreiben kann.

Aufgabe 17.18. (3 Punkte)

Es sei K ein kommutativer Ring. Zeige, dass auf $K[X,X^{-1}] \cong K[X]_X$ durch

$$\begin{aligned}\Delta : K[X,X^{-1}] \longrightarrow K[X,X^{-1}] \otimes_K K[X,X^{-1}] \cong K[X,X^{-1},Y,Y^{-1}],\\ X \longmapsto X \otimes 1 \cdot 1 \otimes X = X \cdot Y,\end{aligned}$$

durch

$$K[X,X^{-1}] \longrightarrow K,\ X \longmapsto 1,$$

und durch

$$K[X,X^{-1}] \longrightarrow K[X,X^{-1}],\ X \longmapsto X^{-1},$$

eine Hopf-Struktur erklärt wird.

18. Vorlesung - Hopf-Algebren und affine Gruppenschemata

In dieser Vorlesung machen wir uns klar, dass das Spektrum einer Hopf-Algebra eine Struktur aufweist, die ähnlich zu einer Gruppe ist, und wir erklären, wie Gruppenoperationen mit Hopfalgebren beschrieben werden können.

Affine Gruppenschemata

Definition 18.1. Es sei K ein kommutativer Ring und H eine kommutative K-Hopf-Algebra. Dann nennt man das Spektrum $G = \operatorname{Spek}(H)$ zusammen mit den induzierten K-Morphismen

$$\Delta^*\colon\ G \times_K G \longrightarrow G,$$
$$\epsilon^*\colon\ \operatorname{Spek}(K) \longrightarrow G$$

und

$$S^*\colon\ G \longrightarrow G$$

das zugehörige *affine Gruppenschema*.

Die Gruppenschemata sind im Allgemeinen keine Gruppen im eigentlichen Sinne, allein schon weil die Primideale, also die Punkte, unterschiedliche Höhe und unterschiedliche Restklassenkörper besitzen. Solche Primideale können nicht sinnvoll miteinander verknüpft werden. Wir werden gleich sehen, dass Punkte, deren Restklassenkörper zusammenpassen, miteinander verknüpft werden können.

Lemma 18.2. *Es sei K ein kommutativer Ring, H eine kommutative Hopf-Algebra und $G = \operatorname{Spek}(H)$ das zugehörige affine Gruppenschema. Dann gelten folgende Aussagen.*

(1) *Die folgenden Diagramme von K-Morphismen kommutieren:*

$$\begin{array}{ccc} G \times_K G \times_K G & \xrightarrow{\Delta^* \times \mathrm{Id}_G} & G \times_K G \\ {\scriptstyle \mathrm{Id}_G \times \Delta^*}\downarrow & & \downarrow{\scriptstyle \Delta^*} \\ G \times_K G & \xrightarrow{\Delta^*} & G \end{array},$$

$$\begin{array}{ccc} G & \xrightarrow{\mathrm{Id} \times (\epsilon^* \iota^*)} & G \times_K G \\ & {\scriptstyle \mathrm{Id}_G}\searrow & \downarrow{\scriptstyle \Delta^*} \\ & & G \end{array},$$

$$\begin{array}{ccc} G & \xrightarrow{S^* \times \mathrm{Id}_G} & G \times_K G \\ {\scriptstyle \iota^*}\downarrow & & \downarrow{\scriptstyle \Delta^*} \\ \operatorname{Spek}(K) & \xrightarrow{\epsilon^*} & G \end{array}$$

(2) *Für jede kommutative K-Algebra L ist $G(L)$ mit den induzierten Operationen eine Gruppe.*

Beweis. (1) folgt unmittelbar aus der Kommutativität der entsprechenden Diagramme für die Hopf-Algebra. (2) folgt aus (1) und aus

$$\begin{aligned} (G \times_K G)(L) &= \operatorname{Hom}_K^{\mathrm{alg}}(H \otimes_K H, L) \\ &= \operatorname{Hom}_K^{\mathrm{alg}}(H, L) \times \operatorname{Hom}_K^{\mathrm{alg}}(H, L) \\ &= G(L) \times G(L), \end{aligned}$$

wobei die mittlere Gleichung auf Satz 17.5 beruht. □

Die vorstehende Aussage erklärt auch teilweise die Bezeichnung Gruppenschema. Einem Gruppenschema ist nicht nur eine Gruppe zugeordnet, sondern gleich eine ganze Familie von Gruppen. Das affine Schema legt dabei die algebraische Struktur der Gruppenverknüpfung fest, während die Anzahl der Elemente in der Gruppe vom gewählten Grundring K abhängt. Wir erläutern das Konzept der K-Punkte an einigen Hopf-Algebren.

Beispiel 18.3. Es sei $(G, 1, \cdot)$ eine endliche Gruppe und K ein Körper. Die gemäß Beispiel 17.8 zugehörige Hopf-Algebra ist einfach $H = \text{Abb}\,(G, K)$, also das $\#(G)$-fache direkte Produkt von K mit sich selbst. Ein K-Algebrahomomorphismus

$$\varphi\colon\ \text{Abb}\,(G, K) \longrightarrow K$$

muss (wegen $e_\sigma \cdot e_\tau = 0$ für $\sigma \neq \tau$) eine Projektion auf eine Komponente sein. D.h. φ muss die Auswertung von $f \in \text{Abb}\,(G, K)$ an einem Gruppenelement $\sigma \in G$ sein. Daher ist

$$K-\text{Spek}\,(\text{Abb}\,(G, K)) = G.$$

Darüber hinaus ist

$$\text{Spek}\,(\text{Abb}\,(G, K)) = K-\text{Spek}\,(\text{Abb}\,(G, K)).$$

Wir identifizieren also Gruppenelemente, Primideale von $\text{Abb}\,(G, K)$ und ihre zugehörigen K-Algebrahomomorphismen (einen Gruppenelement $\sigma \in G$ entspricht die Projektion p_σ auf die σ-Komponente und ihr Kern). Ebenso ist

$$G \times G = K-\text{Spek}\,(H) \times_K K-\text{Spek}\,(H) = K-\text{Spek}\,(H \otimes_K H).$$

Ein Paar $(\sigma, \tau) \in G \times G$ entspricht dabei dem K-Algebrahomomorphismus

$$H \otimes_K H \longrightarrow K,\ f_1 \otimes f_2 \longmapsto \sigma(f_1) \cdot \tau(f_2).$$

Die durch die Hopf-Algebrastruktur induzierte Multiplikation μ auf G von σ und τ, angewendet auf e_ρ, ist

$$\begin{aligned} \mu\,(\sigma, \tau)\,(e_\rho) &= ((\sigma \otimes \tau) \circ \Delta)\,(e_\rho) \\ &= (\sigma \otimes \tau) \left(\sum_{\rho_1 \cdot \rho_2 = \rho} e_{\rho_1} \otimes e_{\rho_2} \right) \\ &= \sum_{\rho_1 \cdot \rho_2 = \rho} \sigma(e_{\rho_1}) \cdot \tau(e_{\rho_2}). \end{aligned}$$

Die Summanden sind nur dann gleich 1 (andernfalls sind sie 0), wenn $\rho_1 = \sigma$ und $\rho_2 = \tau$ ist. Daher ist die Summe nur im Fall

$$\rho = \sigma\tau$$

gleich 1 und sonst gleich 0. Dies bedeutet wiederum

$$\mu(\sigma, \tau) = \sigma\tau,$$

da ja $\sigma\tau$ ebenfalls genau an $e_{\sigma\tau}$ den Wert 1 und sonst überall den Wert 0 besitzt und die K-Algebrahomomorphismen von H nach K auf der Basis

festgelegt sind. Also stimmt die durch die Hopf-Struktur gegebene Multiplikation mit der vorgegebenen Multiplikation überein. Das gleiche gilt für das neutrale Element und die Inversen. Insgesamt gewinnt man also die endliche Gruppe als affines Gruppenschema zur Hopf-Algebra zurück.

Beispiel 18.4. Es sei K ein kommutativer Ring und $H = K[X]$ der Polynomring versehen mit der in Beispiel 17.9 eingeführten (additiven) K-Hopf-Algebrastruktur. Zu einer kommutativen K-Algebra L haben wir die natürliche Bijektion

$$L \longrightarrow \operatorname{Hom}_K^{\mathrm{alg}}(H, L),$$

wobei ein Element $a \in L$ auf den K-Algebrahomomorphismus abgebildet wird, der durch $X \mapsto a$ festgelegt ist. Unter dieser Bijektion wird die durch die Hopf-Struktur induzierte Verknüpfung zur Addition auf L, siehe Aufgabe 18.1. Daher nennt man $\operatorname{Spek}(K[X])$ auch die *additive Gruppe* über K.

Beispiel 18.5. Es sei K ein kommutativer Ring und $H = K[X, X^{-1}] = K[X]_X$ sei mit der in Beispiel 17.10 eingeführten (multiplikativen) K-Hopf-Algebrastruktur versehen. Zu einer kommutativen K-Algebra L haben wir die natürliche Bijektion

$$L^\times \longrightarrow \operatorname{Hom}_K^{\mathrm{alg}}(H, L),$$

wobei eine Einheit $a \in L^\times$ auf den K-Algebrahomomorphismus abgebildet wird, der durch $X \mapsto a$ festgelegt ist. Da a eine Einheit ist, ist dies auf genau eine Weise möglich. Unter dieser Bijektion wird die durch die Hopf-Struktur induzierte Verknüpfung zur Multiplikation auf $L^\times$, siehe Aufgabe 18.6. Daher nennt man $\operatorname{Spek}(K[X, X^{-1}])$ auch die *multiplikative Gruppe* über K.

Beispiel 18.6. Es sei K ein kommutativer Ring und $n \in \mathbb{N}$. Wir möchten eine Hopf-Algebra konstruieren, derart, dass die Menge ihrer K-Punkte mit der induzierten Gruppenstruktur gleich der Gruppe der invertierbaren $n \times n$-Matrizen $\mathrm{GL}_n(K)$ über K ist. Eine solche Matrix besteht aus n^2 Einträgen, von daher betrachten wir zunächst den Polynomring

$$K[X_{ij},\, 1 \leq i, j \leq n].$$

Einen K-Punkt dieses Ringes, also eine Belegung der Variablen, fassen wir als eine Matrix auf. Die Bedingung, dass die Matrix invertierbar ist, kann man über die Determinante ausdrücken, und zwar muss diese eine Einheit in K sein. Eine Belegung der Variablen, die einer invertierbaren Matrix entspricht, muss also aufgrund der universellen Eigenschaft der Nenneraufnahme durch

$$H \;=\; K[X_{ij},\, 1 \leq i, j \leq n]_D$$

faktorisieren, wobei D die Determinante in den Variablen X_{ij} bezeichnet.

Wir erklären auf H eine Hopf-Algebrastruktur, wobei wir uns von der Gruppenstruktur auf der allgemeinen linearen Gruppe leiten lassen. Die Komultiplikation wird durch

$$H \longrightarrow H \otimes_K H,\ X_{ij} \longmapsto \sum_{k=1}^{n} Y_{ik} \otimes Z_{kj},$$

definiert. Die Koeinheit wird durch

$$\epsilon(X_{ij}) = \begin{cases} 1 \text{ für } i = j, \\ 0 \text{ sonst}, \end{cases}$$

festgelegt, das Koinverse wird mit Hilfe der Formel

$$M^{-1} = \frac{1}{\det M} \cdot \text{Adj } M$$

erstellt, wobei die adjungierte Matrix ein Polynom in den Einträgen der Matrix ist. Das Koinverse bildet demnach X_{ij} auf den (i,j)-ten Eintrag in der rechten Seite der obigen Formel ab.

Gernerell gilt, dass man eine Gruppe, die man allein mit algebraischen (polynomialen) Ausdrücken hinschreiben kann, auch durch eine Hopf-Algebra gewinnen kann.

Beispiel 18.7. Die spezielle lineare Gruppe wird als Hopf-Algebra durch

$$H = K[X_{ij},\ 1 \leq i,j \leq n]/(D-1)$$

festgelegt, wobei D die Determinante in den Variablen X_{ij} bezeichnet. Die Komultiplikation, die Koeinheit und das Koinverse sind wie in Beispiel 18.6 zu wählen.

Operationen von affinen Gruppenschemata

Wir wollen nun auch Gruppenoperationen mit Hopf-Algebren ausdrücken. Dabei wird die Menge, auf der operiert wird, ein Spektrum eines kommutativen Ringes sein. Um die Operation richtig algebraisieren zu können, übersetzen wir die Axiome einer Gruppenoperation in die Sprache der kommutativen Diagramme. Eine Gruppenoperation einer Gruppe G auf einer Menge X liegt genau dann vor, wenn die Diagramme (es sei μ die Verknüpfung auf der Gruppe und ν die Operationsabbildung)

$$\begin{array}{ccc} G \times G \times X & \stackrel{\mu \times \mathrm{Id}_X}{\longrightarrow} & G \times X \\ \mathrm{Id}_G \times \nu \downarrow & & \downarrow \nu \\ G \times X & \stackrel{\nu}{\longrightarrow} & X \end{array}$$

und

$$\begin{array}{ccc} X & \stackrel{e\times \mathrm{Id}_X}{\longrightarrow} & G\times X \\ & \mathrm{Id}_X \searrow & \downarrow \nu \\ & & X \end{array}$$

kommutieren.

Definition 18.8. Es sei K ein kommutativer Ring, H eine kommutative K-Hopf-Algebra und R eine kommutative K-Algebra. Unter einer *Kooperation* von H auf R versteht man einen K-Algebrahomomorphismus

$$N\colon\ R \longrightarrow H\otimes_K R$$

derart, dass die beiden Diagramme

$$\begin{array}{ccc} R & \stackrel{N}{\longrightarrow} & H\otimes_K R \\ N\downarrow & & \downarrow \Delta\otimes \mathrm{Id}_R \\ H\otimes_K R & \stackrel{\mathrm{Id}_H\otimes N}{\longrightarrow} & H\otimes_K H\otimes_K R \end{array}$$

und

$$\begin{array}{ccc} R & \stackrel{N}{\longrightarrow} & H\otimes_K R \\ & \cong\searrow & \downarrow \epsilon\otimes \mathrm{Id}_R \\ & & K\otimes_K R \end{array}$$

kommutieren.

Definition 18.9. Es sei K ein kommutativer Ring, H eine kommutative K-Hopf-Algebra und $G = \mathrm{Spek}\,(H)$ das zugehörige affine Gruppenschema. Es sei

$$N\colon\ R \longrightarrow H\otimes_K R$$

eine Kooperation von H auf einem kommutativen Ring R mit dem Spektrum $X = \mathrm{Spek}\,(R)$. Dann nennt man den zu N gehörenden K-Morphismus

$$N^*\colon\ G\times_K X = \mathrm{Spek}\,(H\otimes_K R) \longrightarrow X$$

eine (K-rationale) *Operation des affinen Gruppenschemas* G auf X.

Lemma 18.10. *Es sei K ein kommutativer Ring, H eine kommutative Hopf-Algebra und $G = \mathrm{Spek}\,(H)$ das zugehörige affine Gruppenschema. Es sei R eine weitere kommutative K-Algebra, auf der eine Kooperation von H und damit eine Operation von G auf $X = \mathrm{Spec}\ R$ vorliege. Dann gelten folgende Aussagen (dabei ist $\mu = \triangle^*$, $\nu = N^*$ und j^* bezeichnet den Strukturmorphismus $X \to \mathrm{Spek}\,(K)$).*

(1) *Die folgenden Diagramme von K-Morphismen kommutieren:*

$$\begin{array}{ccc} G \times_K G \times_K X & \stackrel{\mu\times \mathrm{Id}_X}{\longrightarrow} & G \times_K X \\ \mathrm{Id}_G \times \nu \downarrow & & \downarrow \nu \\ G \times_K X & \stackrel{\nu}{\longrightarrow} & X \end{array}$$

und

$$\begin{array}{ccc} X & \stackrel{(\epsilon^* j^*)\times \mathrm{Id}_X}{\longrightarrow} & G \times_K X \\ & \mathrm{Id}_X \searrow & \downarrow \nu \\ & & X \end{array} .$$

(2) *Für jede kommutative K-Algebra L liegt eine Gruppenoperation von $G(L)$ auf $X(L)$ vor.*

Beweis. Dies wird ähnlich wie Lemma 18.2 bewiesen. □

Beispiel 18.11. Zu einem kommutativen Ring K lässt sich die skalare Multiplikation auf dem K^n bzw. auf dem Polynomring $R = K[X_1, \ldots, X_n]$ folgendermaßen als eine Kooperation der Hopf-Algebra $H = K[U, U^{-1}]$ zur multiplikativen Gruppe realisieren: Man definiert die Kooperation durch

$$K[X_1, \ldots, X_n] \longrightarrow K[U, U^{-1}] \otimes_K K[X_1, \ldots, X_n],\ X_i \longmapsto U \otimes X_i.$$

Ein K-Punkt von $H \otimes_K R$ ist dabei nach Satz 17.5 durch einen K-Punkt von H und einen K-Punkt von R gegeben, also durch eine Einheit $t \in K^\times$ und ein n-Tupel $(a_1, \ldots, a_n) \in K^n$ festgelegt. Dieser wird unter der Kooperation wie gewünscht auf $(ta_1, \ldots, ta_n)$ abgebildet.

18. Arbeitsblatt

Aufwärmaufgaben

Aufgabe 18.1. Es sei K ein kommutativer Ring und $H = K[X]$ sei mit der in Beispiel 17.9 eingeführten (additiven) K-Hopf-Algebrastruktur versehen. Zeige, dass zu einer kommutativen K-Algebra L die induzierte Gruppenstruktur auf $L \cong (\mathrm{Spek}\,(H))\,(L)$ mit der Addition auf L übereinstimmt.

Aufgabe 18.2. Es sei K ein kommutativer Ring und H eine kommutative K-Hopf-Algebra zusammen mit einer Kooperation auf der kommutativen K-Algebra R. Wir betrachten die beiden K-Algebrahomomorphismen

$$N\colon\ R \longrightarrow H \otimes_K R$$

(die Kooperation) und

$$\iota_2\colon\ R \longrightarrow H \otimes_K R,\ r \longmapsto 1 \otimes r.$$

Zeige, dass die Menge

$$\{r \in R |\ N(r) = \iota_2(r)\}$$

ein Unterring von R ist.

Den in der vorstehenden Aufgabe definierten Unterring nennt man auch den *Invariantenring der Kooperation*.

Aufgabe 18.3. Es sei X eine Menge, auf der eine Gruppe G operiere, und sei

$$\varphi\colon\ X \longrightarrow Y$$

eine Abbildung in einer weitere Menge Y. Zeige, dass φ genau dann G-invariant ist, wenn das Diagramm

$$G \times X \xrightarrow{\nu, p_2} X \longrightarrow Y$$

kommutiert.

Aufgabe 18.4. Es sei K ein kommutativer Ring und R eine kommutative K-Algebra, auf der eine endliche Gruppe G als Gruppe von K-Algebraautomorphismen operiere.

(1) Definiere eine Kooperation der Hopf-Algebra $H = \text{Abb}\,(G, K)$ auf R derart, dass man über die zugehörige Operation der Spektren die ursprüngliche Operation zurückgewinnt.
(2) Zeige, dass der Invariantenring R^G mit dem Invariantenring zur Kooperation übereinstimmt.

Aufgabe 18.5. Es sei K ein kommutativer Ring, D eine kommutative Gruppe und $K[D]$ der zugehörige Gruppenring mit der in Beispiel 17.11 beschriebenen Hopf-Struktur. Es sei A eine kommutative K-Algebra.

(1) Es liege eine D-Graduierung von A (als K-Algebra) vor. Zeige, dass durch
$$A \longrightarrow K[D] \otimes_K A,\ a_d \longmapsto T^d \otimes a_d,$$
eine K-Kooperation der Hopf-Algebra $K[D]$ auf A festgelegt wird.
(2) Es liege eine K-Kooperation
$$N\colon\ A \longrightarrow K[D] \otimes_K A$$
von $K[D]$ auf A vor. Zeige, dass durch
$$A_d := \left\{a \in A |\, T^d \otimes a = N(a)\right\}$$
eine D-Graduierung auf A festgelegt wird.
(3) Zeige, dass die Zuordnungen aus (1) und (2) invers zueinander sind.

Aufgabe 18.6. Es sei K ein Körper und sei $A = K[X_1, \ldots, X_n]$. Definiere eine Hopf-Algebrastruktur auf A derart, dass zu jeder kommutativen K-Algebra L ein natürlicher Gruppenisomorphismus

$$(\mathrm{Spek}\,(K[X_1, \ldots, X_n]))\,(L) \cong (L^n, +)$$

besteht.

Bei den beiden folgenden Aufgaben denke man an lineare Gleichungen, insbesondere daran, wie sich die Lösungen einer homogenen Gleichung zu den Lösungen einer inhomogenen Gleichung verhalten.

Aufgabe 18.7. Es sei R ein kommutativer Ring, $f_1, \ldots, f_n \in R$ und

$$A = R[T_1, \ldots, T_n]/(f_1T_1 + \ldots + f_nT_n).$$

Definiere eine Hopf-Algebrastrutur auf A (über R).

Aufgabe 18.8. Es sei R ein kommutativer Ring, $f_1, \ldots, f_n, f \in R$. Wir setzen

$$A = R[T_1, \ldots, T_n]/(f_1T_1 + \ldots + f_nT_n),$$

versehen mit der in Aufgabe 18.7 diskutierten Hopf-Algebrastruktur, und

$$B = R[T_1, \ldots, T_n]/(f_1T_1 + \ldots + f_nT_n + f).$$

Definiere eine Kooperation von A auf B (über R).

Aufgaben zum Abgeben

Aufgabe 18.9. (3 Punkte)

Es sei K ein kommutativer Ring und $H = K[X, X^{-1}] = K[X]_X$ sei mit der in Beispiel 17.10 eingeführten (multiplikativen) K-Hopf-Algebrastruktur versehen. Zeige, dass zu einer kommutativen K-Algebra L die induzierte Gruppenstruktur auf $L^\times \cong (\mathrm{Spek}\,(H))\,(L)$ mit der Multiplikation übereinstimmt.

Aufgabe 18.10. (3 Punkte)

Es sei K ein kommutativer Ring, D eine kommutative Gruppe und $K[D]$ der zugehörige Gruppenring. Bestimme zu einer kommutativen K-Algebra L die Gruppe $(\mathrm{Spek}\,(K[D]))\,(L)$.

19. Vorlesung - Formel von Molien

Die Hilbert-Reihe und die Formel von Molien

Wir setzen nun die Untersuchung der Invariantenringe $K[X_1, \ldots, X_n]^G$ zu einer endlichen Gruppe $G \subseteq \mathrm{GL}_n(K)$ fort. Insbesondere wollen wir charakterisieren, wann der Invariantenring ein Polynomring ist, wie das beispielsweise bei der symmetrischen Gruppe der Fall ist. Für diese Fragestellung ist das Konzept der Hilbert-Reihe hilfreich.

Definition 19.1. Es sei K ein Körper und R eine positiv-graduierte kommutative K-Algebra mit der Eigenschaft, dass für jedes $d \in \mathbb{N}$ die Stufe R_d endlichdimensional ist. Dann nennt man die Potenzreihe

$$\sum_{d=0}^{\infty} \dim_K(R_d)\, z^d$$

die *Hilbert-Reihe* von R.

Es handelt sich also um eine Potenzreihe mit Koeffizienten aus $\mathbb{N}$. Wir werden sie als formale Potenzreihe handhaben, Konvergenzuntersuchungen werden keine Rolle spielen. Die Hilbert-Reihe eines Polynomringes, wobei die Variablen positiven Grad besitzen, hat folgende Gestalt.

Lemma 19.2. *Es sei K ein Körper und es sei $R = K[X_1, \ldots, X_n]$ der Polynomring über K, wobei die X_i den positiven Grad $d_i \in \mathbb{N}_+$ haben mögen. Dann ist die Hilbert-Reihe dieses Ringes gleich*

$$H(R,z) = \frac{1}{(1-z^{d_1})\cdots(1-z^{d_n})}.$$

Beweis. Die Monome $X_1^{\nu_1}\cdots X_n^{\nu_n}$ vom Gesamtgrad $d = \sum_{j=1}^n d_j\nu_j$ bilden eine K-Basis von R_d. Die Dimension der d-ten Stufe R_d ist also die Anzahl der Elemente in der Menge

$$A_d := \{(\nu_1, \ldots, \nu_n) \in \mathbb{N}^n \mid \nu_1 d_1 + \ldots + \nu_n d_n = d\}.$$

Die Behauptung folgt somit aus

$$\begin{aligned}
\sum_{d=0}^{\infty} |A_d|\, z^d &= \sum_{d=0}^{\infty} \sum_{(\nu_1,\ldots,\nu_n)\in A_d} z^d \\
&= \left(\sum_{\nu_1=0}^{\infty} z^{\nu_1 d_1}\right)\cdots\left(\sum_{\nu_n=0}^{\infty} z^{\nu_n d_n}\right) \\
&= \frac{1}{1-z^{d_1}}\cdots\frac{1}{1-z^{d_n}},
\end{aligned}$$

wobei wir im letzten Schritt die Formel für die geometrische Reihe verwendet haben. □

Die lineare Operation von einer endlichen Gruppe G auf einem K-Vektorraum V bzw. auf dem zugehörigen Polynomring $R = K[V]$ induziert eine K-lineare Operation $R_d \to R_d$ in jeder Stufe und der Invariantenring R^G ist selbst graduiert. Dies ermöglicht folgende Definition.

Definition 19.3. Die endliche Gruppe G operiere linear auf dem Polynomring $R = K[X_1, \ldots, X_n]$. Dann nennt man die Potenzreihe

$$\Phi_G(z) = \sum_{d=0}^{\infty} \dim_K \left(R_d^G\right) z^d$$

die *Hilbert-Reihe* (oder *Molien-Reihe*) zu dieser Operation.

Die Dimensionen der homogenen Stufen sind endlich und daher ist diese Definition sinnvoll. Die Hilbert-Reihe zur Operation ist einfach die Hilbert-Reihe des Invariantenringes.

Die Dimension des Fixraumes zu einer linearen Operation kann man über die Spur der einzelnen Automorphismen berechnen. Wir erinnern an die Definition der *Spur* einer Matrix und eines Endomorphismus.

Definition 19.4. Es sei K ein Körper und sei $M = (a_{ij})_{ij}$ eine $n \times n$-Matrix über K. Dann heißt

$$\operatorname{Spur}(M) := \sum_{i=1}^{n} a_{ii}$$

die *Spur* von M.

Definition 19.5. Es sei K ein Körper und sei V ein endlichdimensionaler K-Vektorraum. Es sei $\varphi\colon V \to V$ eine lineare Abbildung, die bezüglich einer Basis durch die Matrix M beschrieben werde. Dann nennt man $\operatorname{Spur}(M)$ die *Spur* von φ, geschrieben $\operatorname{Spur}(\varphi)$.

Diese Definition ist unabhängig von der gewählten Basis, siehe Aufgabe 19.5.

Lemma 19.6. *Es sei K ein Körper und V ein endlichdimensionaler K-Vektorraum, auf dem eine endliche Gruppe G linear und treu operiere. Die Gruppenordnung sei kein Vielfaches der Charakteristik von K. Dann besitzt der Fixraum der Operation (also der gemeinsame Eigenraum zum Eigenwert 1) die Dimension*

$$\dim_K \left(V^G\right) = \frac{1}{|G|} \sum_{\sigma \in G} \operatorname{Spur}(\sigma).$$

Beweis. Wir betrachten die lineare Abbildung

$$\pi = \frac{1}{|G|} \sum_{\sigma \in G} \sigma.$$

Zu $w \in V$ ist $\pi(w)$ G-invariant und für $v \in V^G$ ist $\pi(v) = v$. Daher ist π eine lineare Projektion

$$V \longrightarrow V^G.$$

Eine lineare Projektion wird in einer geeigneten Basis durch eine Diagonalmatrix beschrieben, in der $m = \dim_K \left(V^G\right)$ Einsen und sonst Nullen stehen. Also ist $\text{Spur}\,(\pi) = m$. Die Behauptung folgt daraus, dass die Spur additiv ist. $\square$

Der folgende Satz berechnet die Hilbert-Reihe (Formel von Molien).

Satz 19.7. *Es sei K ein algebraisch abgeschlossener Körper der Charakteristik 0. Die endliche Gruppe G operiere linear auf einem endlichdimensionalen K-Vektorraum V. Dann ist*

$$\Phi_G(z) \;=\; \frac{1}{|G|} \sum_{\sigma \in G} \frac{1}{\det\,(\mathrm{Id} - z\sigma)}.$$

Beweis. Der lineare Automorphismus σ ist nach Satz 3.19 diagonalisierbar, da er endliche Ordnung hat. In einer geeigneten Basis besitzt die duale Abbildung σ^* die Gestalt

$$X_i \longmapsto \xi_i X_i\,.$$

Auf der d-ten Stufe induziert dies den linearen Automorphismus

$$\sigma^{(d)}\colon\; K[V]_d \longrightarrow K[V]_d$$

mit $X^\nu \longmapsto \xi^\nu X^\nu$. Die Eigenvektoren von $\sigma^{(d)}$ sind die $\binom{n+d-1}{d}$ verschiedenen Monome

$$X_1^{\nu_1} \cdots X_n^{\nu_n}$$

(es sei $n = \dim_K (V)$) mit $\nu_1 + \ldots + \nu_n = d$ mit den Eigenwerten $\xi_1^{\nu_1} \cdots \xi_n^{\nu_n}$. Die Spur von $\sigma^{(d)}$ ist daher

$$\text{Spur}\left(\sigma^{(d)}\right) \;=\; \sum_{|\nu|=d} \xi^\nu.$$

Nach Lemma 19.6 ergibt sich

$$\dim_K \left(K[V]_d^G\right) \;=\; \frac{1}{|G|} \sum_{\sigma \in G} \text{Spur}\left(\sigma^{(d)}\right)$$

mit

$$\text{Spur}\left(\sigma^{(d)}\right) \;=\; \sum_{\nu_1+\ldots+\nu_n=d} \xi_1^{\nu_1} \cdots \xi_n^{\nu_n}.$$

Damit ist unter Verwendung der geometrischen Reihe

$$\begin{aligned} \Phi_G(z) \;&=\; \sum_{d=0}^{\infty} \left(\frac{1}{|G|} \sum_{\sigma \in G} \text{Spur}\left(\sigma^{(d)}\right) \right) z^d \\ &=\; \frac{1}{|G|} \sum_{d=0}^{\infty} \left(\sum_{\sigma \in G} \sum_{\nu_1+\ldots+\nu_n=d} \xi_{\sigma,1}^{\nu_1} \cdots \xi_{\sigma,n}^{\nu_n} \right) z^d \end{aligned}$$

$$
\begin{aligned}
&= \frac{1}{|G|} \sum_{\sigma\in G} \sum_{(\nu_1,\ldots,\nu_n)\in\mathbb{N}^n} \xi_{\sigma,1}^{\nu_1} \cdots \xi_{\sigma,n}^{\nu_n} z^{\nu_1+\ldots+\nu_n} \\
&= \frac{1}{|G|} \sum_{\sigma\in G} \left(\sum_{\nu_1=0}^{\infty} \xi_{\sigma,1}^{\nu_1} z^{\nu_1} \right) \cdots \left(\sum_{\nu_n=0}^{\infty} \xi_{\sigma,n}^{\nu_n} z^{\nu_n} \right) \\
&= \frac{1}{|G|} \sum_{\sigma\in G} \frac{1}{(1-z\xi_{\sigma,1}) \cdots (1-\xi_{\sigma,n})} \\
&= \frac{1}{|G|} \sum_{\sigma\in G} \frac{1}{\det\,(\mathrm{Id} - z\sigma)}.
\end{aligned}
$$

□

Die Formel besagt insbesondere, dass diese Potenzreihe eine rationale Funktion (also ein Quotient aus zwei Polynomen) ist und daher nur endlich viele Polstellen hat. Die Nennerpolynome in den Summanden erinnern an die charakteristischen Polynome der Gruppenelemente, doch steht hier die Variable bei der linearen Abbildung, nicht bei der Identität.

Der Satz von Chevalley-Shephard-Todd

Wir wenden uns nun der Charakterisierung derjenigen linearen Operationen auf dem Polynomring zu, die zu einem Invariantenring führen, der selbst ein Polynomring ist.

Definition 19.8. Ein linearer Automorphismus auf einem endlichdimensionalen K-Vektorraum heißt *Pseudoreflektion* (oder *Pseudospiegelung*), wenn er in einer geeigneten Basis durch eine Matrix der Form

$$
\begin{pmatrix}
1 & 0 & \cdots & \cdots & 0 \\
0 & 1 & 0 & \cdots & 0 \\
\vdots & \ddots & \ddots & \ddots & \vdots \\
0 & \cdots & 0 & 1 & 0 \\
0 & \cdots & \cdots & 0 & \zeta
\end{pmatrix},
$$

wobei $\zeta \neq 1$ eine Einheitswurzel ist, beschrieben werden kann.

Eine Pseudoreflektion besitzt also eine Hyperebene (einen $(n-1)$-dimensionalen Untervektorraum), auf der sie fix ist (der Eigenraum zum Eigenwert 1) und einen weiteren dazu linear unabhängigen Eigenvektor zum Eigenwert ζ. Die Ordnung der Einheitswurzel ζ bestimmt auch die Ordnung der Pseudoreflektion. Das Inverse einer Pseudoreflektion ist wieder eine Pseudoreflektion.

Definition 19.9. Eine endliche Untergruppe $G \subseteq \mathrm{GL}_n(K)$ heißt *Reflektionsgruppe* (oder *Spiegelungsgruppe*), wenn sie durch Pseudoreflektionen erzeugt wird.

Man beachte, dass dies keine Eigenschaft der (abstrakten) Gruppe G ist, sondern eine Eigenschaft der Untergruppe $G \subseteq \mathrm{GL}_n(K)$. In einer Reflektionsgruppe kann man jedes Element τ als ein Produkt $\tau = \sigma_1 \cdots \sigma_k$ mit Pseudoreflektionen σ_j schreiben.

Die Bedeutung von Reflektionsgruppen in der Invariantentheorie kommt im folgenden wichigen Satz, dem *Satz von Chevalley-Shephard-Todd*, zum Ausdruck.

Satz 19.10. *Es sei K ein algebraisch abgeschlossener Körper der Charakteristik null. Die endliche Gruppe G operiere linear und treu auf dem K-Vektorraum V. Dann sind folgende Aussagen äquivalent.*

(1) *$G \subseteq \mathrm{GL}_n(K)$ ist eine Reflektionsgruppe.*
(2) *Der Invariantenring $K[X_1, \ldots, X_n]^G$ ist (isomorph zu einem) ein Polynomring (in n Variablen).*

Aus Dimensionsgründen ist klar, dass wenn der Invariantenring ein Polynomring ist, dieser n Variablen besitzt. Der Beweis dieses Satzes benutzt verschiedene Lemmata und verwendet die Theorie der Hilbert-Reihen. Hierbei werden verschiedene elementare Hilfsmittel aus der Theorie der Potenzreihen verwendet.

Lemma 19.11. *Es sei K ein algebraisch abgeschlossener Körper und $\sigma \in \mathrm{GL}_n(K)$ eine Pseudoreflektion. Es sei H_σ der Fixraum zu σ und L_σ eine Linearform $\neq 0$, die auf H_σ verschwindet. Dann ist L_σ für jedes Polynom $f \in K[X_1, \ldots, X_n]$ ein Teiler von $f\sigma - f$.*

Beweis. Für $v \in H_\sigma$ ist

$$(f\sigma - f)(v) = f(\sigma v) - f(v) = f(v) - f(v) = 0.$$

Das Polynom $f\sigma - f$ verschwindet also auf der Nullstellenmenge von L_σ. Wir können L_σ zu einer Variablenmenge $L_\sigma, L_2, \ldots, L_n$ ergänzen und

$$f\sigma - f = P(L_\sigma, L_2, \ldots, L_n)L_\sigma + Q(L_2, \ldots, L_n)$$

schreiben. Das Polynom Q verschwindet auf H_σ und ist somit die Nullfunktion, also muss es auch das Nullpolynom sein, da der Körper unendlich ist. □

Lemma 19.12. *Es sei K ein algebraisch abgeschlossener Körper der Charakteristik 0 und $G \subseteq \mathrm{GL}_n(K)$ eine Reflektionsgruppe. Es sei I_G das Ideal in $K[X_1, \ldots, X_n]$, das durch die homogenen Invarianten von einem positiven Grad erzeugt wird. Es gelte*

$$g_1 h_1 + \ldots + g_m h_m = 0,$$

wobei die $h_1, \ldots, h_m \in K[X_1, \ldots, X_n]$ homogene Polynome und die $g_1, \ldots, g_m \in K[X_1, \ldots, X_n]^G$ invariante Polynome seien. Dann ist $h_1 \in I_G$ oder $g_1 \in (g_2, \ldots, g_m)$.

Beweis. Wir führen Induktion über den Grad von h_1. Bei $h_1 = 0$ gehört natürlich h_1 zu I_G. Für $h_1 \neq 0$ und $\operatorname{grad}(h_i) = 0$ ist $g_1 \in (g_2, \ldots, g_m)$. Sei also $\operatorname{grad}(h_1) \geq 1$ und die Aussage für kleineren Grad bewiesen. Es sei $g_1 \notin (g_2, \ldots, g_m)$ vorausgesetzt und es sei $\sigma \in G$ eine Pseudoreflektion. Dann ist

$$\sum_{i=1}^{m} g_i \cdot (h_i \sigma) = \left(\sum_{i=1}^{m} g_i h_i \right) \sigma = 0\sigma = 0.$$

Nach Lemma 19.11 kann man

$$h_i \sigma = h_i + L_\sigma \cdot \widetilde{h}_i$$

schreiben, wobei L_σ eine beschreibende Linearform des Fixraumes zu σ ist und $\widetilde{h}_i$ einen kleineren Grad als h_i besitzt. Wir schreiben die obige Gleichung als

$$0 = \sum_{i=1}^{m} g_i \left(h_i + L_\sigma \widetilde{h}_i \right) = L_\sigma \sum_{i=1}^{m} g_i \widetilde{h}_i.$$

Daher ist die Summe rechts gleich 0 und nach Induktionsvoraussetzung ist $\widetilde{h}_1 \in I_G$, also auch $h_1\sigma - h_1 = \widetilde{h}_1 L_\sigma \in I_G$.

Sei nun $\tau = \sigma_1 \cdots \sigma_k \in G$ ein Produkt von Pseudoreflektionen. Dann ist

$$\begin{aligned} h_1\tau - h_1 &= \sum_{i=1}^{k} (h_1\sigma_i \cdots \sigma_k - h_1\sigma_{i+1} \cdots \sigma_k) \\ &= \sum_{i=1}^{k} (h_1\sigma_i - h_1)(\sigma_{i+1} \cdots \sigma_k). \end{aligned}$$

Da $h_1\sigma_i - h_1$ zu I_G gehört und I_G unter G invariant ist, gehört auch $h_1\tau - h_1$ zu I_G. Mit dem Reynolds-Operator ρ ist

$$\rho(h_1) - h_1 = \left(\frac{1}{|G|} \sum_{\tau \in G} h_1\tau \right) - h_1 = \frac{1}{|G|} \sum_{\tau \in G} (h_1\tau - h_1).$$

Dies gehört zu I_G und wegen $\rho(h_1) \in I_G$ ist auch $h_1 \in I_G$. □

19. Arbeitsblatt

Aufwärmaufgaben

Aufgabe 19.1. Es sei $M \subseteq \mathbb{Z}^n$ ein normales, spitzes, endlich erzeugtes Monoid und K ein Körper. Zeige, dass der Monoidring $K[M]$ eine positive Graduierung besitzt.

Aufgabe 19.2. Bestimme die Hilbert-Reihe von $K[X,Y]/(X^3, Y^5, X^2Y^2)$ in der Standardgraduierung.

Aufgabe 19.3. Es sei K ein Körper und seien A und B endlich erzeugte positiv-graduierte K-Algebren. Zeige, dass zwischen den Hilbert-Reihen die Beziehung

$$H(A \otimes_K B) \, = \, H(A) \cdot H(B)$$

besteht, wobei $A \otimes_K B$ mit der natürlichen $\mathbb{N}$-Graduierung (wie sieht die aus?) versehen sei.

Aufgabe 19.4. Es sei K ein Körper und sei R eine endlich erzeugte, kommutative, positiv-graduierte K-Algebra und $\ell \in \mathbb{N}$. Welche Beziehung besteht zwischen der Hilbert-Reihe von R und der Hilbert-Reihe des ℓ-ten Veronese-Ringes $R^{(\ell)}$.

Aufgabe 19.5. Zeige, dass die Definition 19.5 der Spur einer linearen Abbildung unabhängig von der gewählten Matrix ist.

Aufgabe 19.6. Es sei K ein Körper und sei V ein endlichdimensionaler K-Vektorraum. Zeige, dass die Zuordung

$$\operatorname{End}(V) \longrightarrow K, \, \varphi \longmapsto \operatorname{Spur}(\varphi),$$

K-linear ist.

Aufgabe 19.7. Es sei K ein Körper und sei M eine $n \times n$-Matrix über K. Wie findet man die $\operatorname{Spur}(M)$ im charakteristischen Polynom χ_M wieder?

Aufgabe 19.8. Es sei K ein Körper und sei M eine $n \times n$-Matrix über K mit der Eigenschaft, dass das charakteristische Polynom in Linearfaktoren zerfällt, also

$$\chi_M = (X - \lambda_1)^{\mu_1} \cdot (X - \lambda_2)^{\mu_2} \cdots (X - \lambda_k)^{\mu_k} .$$

Zeige, dass

$$\operatorname{Spur}(M) = \sum_{i=1}^{k} \mu_i \lambda_i$$

ist.

Aufgabe 19.9. Sei K ein Körper und sei $P = X^n - c \in K[X]$ ein irreduzibles Polynom. Es sei

$$f \, = \, a_{n-1}X^{n-1} + a_{n-2}X^{n-2} + \ldots + a_1 X + a_0$$

ein Element in der einfachen endlichen Körpererweiterung $K \subseteq L = K[X]/(P)$ vom Grad n. Zeige, dass die Spur von f (aufgefasst als Endomorphismus auf L) gleich na_0 ist.

Aufgabe 19.10. Zeige, dass man jede endliche zyklische Gruppe $\mathbb{Z}/(n)$ in $\mathrm{GL}_2(\mathbb{C})$ sowohl als Reflektionsgruppe als auch als eine Gruppe ohne Pseudoreflektionen realisieren kann.

Aufgabe 19.11. Zeige, dass die alternierende Gruppe A_n in ihrer natürlichen Realisierung in $\mathrm{GL}_n(K)$ keine Pseudoreflektionen enthält.

Aufgabe 19.12. Es sei K ein Körper und es sei $\psi \in \mathrm{GL}_n(K)$ eine Pseudoreflektion. Zeige, dass jede Konjugation von ψ ebenfalls eine Pseudoreflektion ist.

Aufgabe 19.13. Es sei K ein Körper, $G \subseteq \mathrm{GL}_n(K)$ eine Untergruppe und $H \subseteq G$ die von allen Pseudoreflektionen in G erzeugte Untergruppe. Zeige, dass H ein Normalteiler in G ist.

Aufgaben zum Abgeben

Aufgabe 19.14. (3 Punkte)

Es sei K ein Körper und sei R eine endlich erzeugte, kommutative, positivgraduierte K-Algebra. Zeige, dass die Hilbert-Reihe von R genau dann ein Polynom ist, wenn die Krulldimension von R null ist.

Aufgabe 19.15. (2 Punkte)

Begründe mit dem Satz von Chevalley-Shephard-Todd, dass der Ring der symmetrischen Polynome ein Polynomring ist.

20. Vorlesung - Regularität

Beweis der Hinrichtung

Wir kommen zum *Beweis der Hinrichtung* im Satz von Chevalley-Shephard-Todd, d.h. wir zeigen, dass eine Spiegelungsgruppe einen Polynomring als Invariantenring besitzt. Wir werden wiederholt mit partiellen formalen Ableitungen arbeiten. Diese verhalten sich wie die üblichen partiellen Ableitungen über $\mathbb{R}$ oder über $\mathbb{C}$.

Definition 20.1. Es sei K ein Körper. Zu einem Polynom

$$F = \sum_{\nu} a_\nu X^\nu \in K[X_1, \ldots, X_n]$$

und i, $1 \leq i \leq n$, heißt das Polynom

$$\frac{\partial F}{\partial X_i} := \sum_{\nu} \nu_i a_\nu X_1^{\nu_1} \cdots X_{i-1}^{\nu_{i-1}} X_i^{\nu_i - 1} X_{i+1}^{\nu_{i+1}} \cdots X_n^{\nu_n}$$

die *formale partielle Ableitung* von F nach X_i.

Wir beweisen nun die Hinrichtung.

Beweis. Wir betrachten das Ideal $I_G \subseteq K[X_1, \ldots, X_n]$, das von allen homogenen invarianten Polynomen positiven Grades erzeugt wird. Es sei $I_G = (f_1, \ldots, f_m)$ ein homogenes minimales Erzeugendensystem für dieses Ideal. Aufgrund von Lemma 12.6 bilden diese $f_1, \ldots, f_m$ ein Algebraerzeugendensystem von $K[X_1, \ldots, X_n]^G$. Wir zeigen, dass die f_i algebraisch unabhängig sind und nehmen an, dass $g(f_1, \ldots, f_m) = 0$ ist mit $g \in K[Y_1, \ldots, Y_m]$, $g \neq 0$, ist. Sei dabei g von minimalem Grad.

Das Monom Y^ν aus g wird nach Einsetzen zu f^ν, was ein homogenes Polynom vom Grad $\sum_i \nu_i \operatorname{grad}(f_i)$ ist. Wir können daher annehmen, dass alle Monome, die in $g(f_1, \ldots, f_m)$ vorkommen, den gemeinsamen Grad d haben (die Monome, die zu einem anderen Grad führen, werden einfach weggelassen).

Wir betrachten

$$g_i := \frac{\partial g}{\partial y_i}(f_1, \ldots, f_m),$$

die zum Invariantenring $K[X_1, \ldots, X_n]^G$ gehören. Die g_i sind 0 oder sie haben den Grad $d - \operatorname{grad}(f_i)$. Da $g(y_1, \ldots, y_m)$ nicht konstant ist, ist

$$\frac{\partial g}{\partial y_i}(y_1, \ldots, y_m) \neq 0$$

für zumindest ein i, da wir Charakteristik 0 voraussetzen. Dann muss auch $g_i \neq 0$ für ein i sein, da g nach Annahme minimalen Grad besitzt.

Wir betrachten das Ideal $J = (g_1, \ldots, g_m) \subseteq K[X_1, \ldots, X_n]$, und sei nach Umnummerierung k (≥ 1) so gewählt, dass

$$J = (g_1, \ldots, g_k)$$

ist, aber keine echte Teilmenge davon dieses Ideal erzeugt. Für $i > k$ schreiben wir

$$g_i = \sum_{j=1}^{k} h_{ij} g_j,$$

wobei $h_{ij} = 0$ ist oder aber homogen vom Grad $\operatorname{grad}(g_i) - \operatorname{grad}(g_j) = \operatorname{grad}(f_j) - \operatorname{grad}(f_i)$. Es folgt

$$\begin{aligned} 0 &= \frac{\partial}{\partial x_s}\left(g\left(f_1,\ldots,f_m\right)\right) \\ &= \sum_{i=1}^{m} g_i \frac{\partial f_i}{\partial x_s} \\ &= \sum_{i=1}^{k} g_i \frac{\partial f_i}{\partial x_s} + \sum_{i=k+1}^{m} \left(\sum_{j=1}^{k} h_{ij} g_j\right) \frac{\partial f_i}{\partial x_s} \\ &= \sum_{i=1}^{k} g_i \left(\frac{\partial f_i}{\partial x_s} + \sum_{j=k+1}^{m} \left(h_{ji} \frac{\partial f_j}{\partial x_s}\right)\right). \end{aligned}$$

Wegen $g_1 \notin (g_2,\ldots,g_k)$ gehört für jedes s das homogene Element

$$\frac{\partial f_1}{\partial x_s} + \sum_{j=k+1}^{m} h_{j1} \frac{\partial f_j}{\partial x_s}$$

nach Lemma 19.12 zu I_G. Daraus ergibt sich durch Multiplikation mit x_s

$$\begin{aligned} \sum_{s=1}^{n} x_s \frac{\partial f_1}{\partial x_s} + \sum_{j=k+1}^{m} h_{j1} \sum_{s=1}^{n} x_s \frac{\partial f_j}{\partial x_s} &= \left(\operatorname{grad}(f_1)\right) f_1 + \sum_{j=k+1}^{m} h_{j1} \left(\operatorname{grad}(f_j)\right) f_j \\ &\in (x_1,\ldots,x_n) I_G \\ &\subseteq (x_1 f_1,\ldots,x_n f_1) + (f_2,\ldots,f_m). \end{aligned}$$

Die hinteren Summanden in diesem Polynom gehören zu $(f_2,\ldots,f_m)$, daher ist

$$f_1 \in (x_1 f_1,\ldots,x_n f_1) + (f_2,\ldots,f_m).$$

Aus Gradgründen ist $f_1 \in (f_2,\ldots,f_m)$, was ein Widerspruch zur Minimalität des Idealerzeugendensystems von I_G ist. □

Laurent-Entwicklung der Hilbert-Reihe

Wir wenden uns nun der *Rückrichtung* im Satz von Chevalley-Shephard-Todd zu. Zuerst erinnern wir an die *Laurent-Entwicklung*. Eine rationale Funktion besitzt eine Laurent-Entwicklung

$$Q(z) = \frac{F(z)}{G(z)} = \sum_{i=k}^{\infty} a_i z^i,$$

wobei k eine eventuell negative Zahl ist. Ist $a_k \neq 0$ und k minimal und negativ, so heißt $-k$ die Polstellenordnung ($\frac{1}{z^k}$ hat einen Pol der Ordnung k).

Lemma 20.2. *Es sei K ein algebraisch abgeschlossener Körper der Charakteristik 0. Es sei $G \subset \mathrm{GL}_n(K)$ eine endliche Untergruppe und sei r die Anzahl der Pseudoreflektionen in G. Dann ist die Laurent-Entwicklung der Hilbert-Reihe des Invariantenringes um $z = 1$ gleich*

$$\Phi_G(z) = \frac{1}{|G|}(1-z)^{-n} + \frac{r}{2\,|G|}(1-z)^{-n+1} + \dots .$$

Beweis. Nach der Molien-Formel ist

$$\Phi_G(z) = \frac{1}{|G|}\sum_{\sigma\in G}\frac{1}{\det\,(\mathrm{Id} - z\sigma)}.$$

Die Summanden haben die Gestalt

$$\frac{1}{|G|}\frac{1}{\det\,(\mathrm{Id} - z\sigma)} = \frac{1}{|G|}\frac{1}{(1-z\xi_{\sigma,1})}\cdots\frac{1}{(1-z\xi_{\sigma,n})},$$

wobei die $\xi_{\sigma,j}$ die Eigenwerte (mit Wiederholungen) von σ seien. Für $\sigma = \mathrm{Id}$ hat der entsprechende Summand in $z = 1$ einen Pol der Ordnung n. Für $\sigma \neq \mathrm{Id}$ haben die Summanden an $z = 1$ einen Pol von maximaler Ordnung $n-1$. Diese Maximalität tritt genau dann ein, wenn der Eigenwert 1 die Vielfachheit $n-1$ besitzt, wenn also σ eine Pseudoreflektion ist. In diesem Fall ist

$$\frac{1}{\det\,(\mathrm{Id} - z\sigma)} = \frac{1}{(1-z)^{n-1}}\cdot\frac{1}{(1-z\det\,\sigma)},$$

da bei einer Pseudoreflektion der andere Eigenwert gleich der Determinante ist. Daher ist der Koeffizient zu $(1-z)^{-n+1}$ in der Laurent-Entwicklung gleich

$$\frac{1}{|G|}\sum_{\sigma\text{ Pseudoreflektion}}\frac{1}{1-\det\,\sigma}$$

(im hinteren Faktor wird $z = 1$ gesetzt). Das Inverse einer Pseudoreflektion ist ebenfalls eine Pseudoreflektion, daher ist

$$\begin{aligned} 2\sum_{\sigma\text{ Pseudoreflektion}}\frac{1}{1-\det\,\sigma} &= \sum_{\sigma\text{ Pseudoreflektion}}\left(\frac{1}{1-\det\,\sigma} + \frac{1}{1-(\det\,\sigma)^{-1}}\right) \\ &= \sum_{\sigma\text{ Pseudoreflektion}} 1 \\ &= r. \end{aligned}$$

□

Beweis der Rückrichtung

Wir beweisen nun die Rückrichtung des Satzes von Chevalley-Sheppard-Todd, dass also ein algebraisch unabhängiges Algebraerzeugendensystem nur bei einer Reflektionsgruppe vorliegen kann. Die Strategie ist, die von den

Pseudoreflektionen erzeugte Untergruppe $H \subseteq G$ zu untersuchen und dabei letztlich auf $H = G$ zu schließen.

Korollar 20.3. *Es sei K ein algebraisch abgeschlossener Körper der Charakteristik 0. Es sei $G \subseteq \mathrm{GL}_n(K)$ eine endliche Gruppe derart, dass der zugehörige Invariantenring von n algebraisch unabhängigen homogenen Invarianten $\theta_1, \ldots, \theta_n$ erzeugt werde. Es sei $d_i = \mathrm{grad}(\theta_i)$ und r die Anzahl der Pseudoreflektionen in G. Dann ist*

$$|G| = d_1 \cdots d_n \text{ und } r = d_1 + \ldots + d_n - n\,.$$

Beweis. Nach Lemma 19.2 ist

$$\Phi_G(z) \;=\; \frac{1}{(1-z^{d_1})} \cdots \frac{1}{(1-z^{d_n})}.$$

Wegen $1 - z^d = (1-z)\left(1 + z + \ldots + z^{d-1}\right)$ ist dies gleich

$$\frac{1}{(1-z)^n} \cdot \frac{1}{1+z+\ldots+z^{d_1-1}} \cdots \frac{1}{1+z+\ldots+z^{d_n-1}}\,.$$

Der Bruch $\frac{1}{1+z+\ldots+z^{d-1}}$ hat um $z = 1$ die Potenzreihenentwicklung

$$\frac{1}{d} - \frac{d-1}{2d}(z-1) + \ldots\,,$$

was sich durch Einsetzen und Ableiten ergibt. Die Laurent-Entwicklung um $z = 1$ ergibt sich durch Einsetzen zu

$$\Phi_G(z) \;=\; \frac{1}{d_1 \cdots d_n}(1-z)^{-n} + \frac{d_1 + \ldots + d_n - n}{2d_1 \cdots d_n}(1-z)^{-n+1} + \ldots.$$

Der Vergleich mit Lemma 20.2 ergibt die Behauptung. □

Wir beweisen nun die Rückrichtung im Satz von Chevalley-Shephard-Todd.

Beweis. Es sei

$$K[X_1, \ldots, X_n]^G \;=\; K[\theta_1, \ldots, \theta_n]$$

mit θ_i algebraisch unabhängig, und es sei $\mathrm{grad}(\theta_i) = d_i$. Es sei $H \subseteq G$ die durch alle Pseudoreflektionen erzeugte Untergruppe. Aufgrund der Hinrichtung des Satzes von Chevalley-Shephard-Todd wissen wir bereits

$$K[X_1, \ldots, X_n]^H \;=\; K[\psi_1, \ldots, \psi_n] \;\supseteq\; K[X_1, \ldots, X_n]^G$$

mit $\mathrm{grad}(\psi_j) = e_j$ und ψ_j algebraisch unabhängig. Jedes θ_i ist ein Polynom in den ψ_j. Wir können annehmen, dass beide Polynomfamilien nach aufsteigendem Grad geordnet sind, es ist also $d_1 \leq d_2 \leq \ldots \leq d_n$ und $e_1 \leq e_2 \leq \ldots \leq e_n$. Dabei muss

$$e_i \;\leq\; d_i$$

für alle i gelten, da andernfalls nach Aufgabe 20.12

$$K[\theta_1, \ldots, \theta_i] \;\subseteq\; K[\psi_1, \ldots, \psi_{i-1}]$$

gelten würde, was aber wegen der algebraischen Unabhängigkeit der Familien nicht sein kann. Es sei r die Anzahl der Pseudoreflektionen in G und in H. Nach Korollar 20.3 ist

$$r \;=\; \sum_{i=1}^{n}(d_i - 1) \;=\; \sum_{i=1}^{n}(e_i - 1).$$

Daher muss $e_i = d_i$ gelten. Damit ist aber

$$|G| \;=\; d_1 \cdots d_n \;=\; e_1 \cdots e_n \;=\; |H|$$

und damit

$$H = G\,.$$

□

20. Arbeitsblatt

Aufwärmaufgaben

Aufgabe 20.1. Überprüfe Korollar 20.3 für die symmetrische Gruppe.

Aufgabe 20.2. Zeige, dass die spezielle lineare Gruppe $\mathrm{SL}_n(K)$ keine Pseudoreflektionen enthält.

Aufgabe 20.3. Es sei K ein Körper, $\sigma \in \mathrm{GL}_n(K)$ eine Pseudoreflektion und G die von σ erzeugte zyklische Gruppe. Zeige direkt, dass der Invariantenring $K[X_1, \ldots, X_n]^G$ ein Polynomring ist.

Aufgabe 20.4. Man gebe ein Beispiel für eine Reflektionsgruppe G und eine nichttrivale Untergruppe $H \subseteq G$, die keine Pseudoreflektion enthält.

Aufgabe 20.5. Wir betrachten die symmetrische Gruppe S_n mit ihrer natürlichen Einbettung $S_n \subseteq \mathrm{GL}_n(K)$ über einem Körper K. Zeige, dass $\sigma \in S_n$ genau dann eine Transposition ist, wenn σ eine Pseudoreflektion ist.

Aufgabe 20.6. Zeige, dass der Polynomring $K[X_1, \ldots, X_n]$ ein freier Modul über dem Polynomring $K[E_1, \ldots, E_n]$ der elementarsymmetrischen Polynome ist.

Aufgabe 20.7. Sei K ein Körper und sei $K[X]$ der Polynomring über K. Beweise die folgenden Rechenregeln für das formale Ableiten $F \mapsto F'$:

(1) Die Ableitung eines konstanten Polynoms ist null.
(2) Die Ableitung ist K-linear.
(3) Es gilt die *Produktregel*, also

$$(FG)' = FG' + F'G\,.$$

Aufgabe 20.8. Sei K ein Körper und sei $K[X]$ der Polynomring über K. Es sei $F \in K[X]$ und $a \in K$. Zeige, dass a genau dann eine mehrfache Nullstelle von F ist, wenn $F'(a) = 0$ ist, wobei F' die formale Ableitung von F bezeichnet.

Aufgabe 20.9. Sei K ein Körper der Charakteristik $p \geq 0$. Man charakterisiere die Polynome $F \in K[X,Y]$ mit der Eigenschaft, dass

(1) die erste partielle Ableitung,
(2) die zweite partielle Ableitung,
(3) beide partiellen Ableitungen

null sind.

Aufgabe 20.10. Es sei $H \in K[X_1, \ldots, X_n]$ ein (in der Standardgraduierung) homogenes Polynom vom Grad e. Zeige die Beziehung

$$eH \;=\; X_1 \frac{\partial H}{\partial X_1} + \ldots + X_n \frac{\partial H}{\partial X_n}.$$

Aufgabe 20.11. Es sei K ein Körper und seien $F_1, \ldots, F_m \in K[X_1, \ldots, X_n]$ und $G_1, \ldots, G_k \in K[Y_1, \ldots, Y_m]$ Polynome. Wir setzen

$$H_i \;=\; G_i(F_1, \ldots, F_m).$$

Dann gilt für die formalen partiellen Ableitungen die „formale Kettenregel“

$$\begin{pmatrix} \frac{\partial H_1}{\partial X_1} & \cdots & \frac{\partial H_1}{\partial X_n} \\ \vdots & \ddots & \vdots \\ \frac{\partial H_k}{\partial X_1} & \cdots & \frac{\partial H_k}{\partial X_n} \end{pmatrix} = \begin{pmatrix} \frac{\partial G_1}{\partial Y_1} & \cdots & \frac{\partial G_1}{\partial Y_m} \\ \vdots & \ddots & \vdots \\ \frac{\partial G_k}{\partial Y_1} & \cdots & \frac{\partial G_k}{\partial Y_m} \end{pmatrix} \begin{pmatrix} F_j \\ Y_j \end{pmatrix} \circ \begin{pmatrix} \frac{\partial F_1}{\partial X_1} & \cdots & \frac{\partial F_1}{\partial X_n} \\ \vdots & \ddots & \vdots \\ \frac{\partial F_m}{\partial X_1} & \cdots & \frac{\partial F_m}{\partial X_n} \end{pmatrix}.$$

Aufgabe 20.12. Es sei K ein Körper und $R = K[X_1, \ldots, X_n]$ der Polynomring mit der Standardgraduierung. Es seien $Q, P_1, \ldots, P_m \in R$ homogene Polynome mit

$$Q \in K[P_1, \ldots, P_m]\,.$$

Zeige $Q \in K[P_j,\, j \in J]$, wobei der Grad der P_j, $j \in J$, maximal gleich dem Grad von Q ist.

Aufgaben zum Abgeben

Aufgabe 20.13. (3 Punkte)

Man gebe ein Beispiel für eine zyklische Reflektionsgruppe derart, dass die Erzeuger der Gruppe keine Pseudoreflektionen sind.

Aufgabe 20.14. (5 Punkte)

Wie viele Pseudoreflektionen enthält die allgemeine lineare Gruppe $\mathrm{GL}_2(\mathbb{F}_3)$ über dem Körper $\mathbb{F}_3$ mit drei Elementen.

Die folgende Aussabe kann man bei $K = \mathbb{C}$ mit dem Satz von Chevalley (der besagt, dass Bilder „konstruierbarer Mengen“ wieder konstruierbar sind) und der Transformationsformel für Volumina beweisen. Gibt es auch einen elementaren algebraischen Beweis?

Aufgabe 20.15. (10 Punkte)

Es sei K ein Körper der Charakteristik 0 und seien $Q_1, \ldots, Q_n \in K[X_1, \ldots, X_n]$ algebraisch unabhängige Polynome. Zeige

$$\det\left(\left(\frac{\partial Q_i}{\partial X_j}\right)_{ij}\right) \neq 0.$$

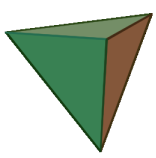
21. Vorlesung - Symmetriegruppen I

In den folgenden Vorlesungen werden wir die endlichen Untergruppen $G \subseteq \mathrm{SL}_2(\mathbb{C})$ und ihre Invariantenringe klassifizieren. Dieses Klassifikationsproblem hängt mit einem klassischen und anschaulichen Problem zusammen, nämlich der Frage, welche endlichen Symmetriegruppen es im euklidischen dreidimensionalen Raum gibt. Diese Gruppen haben mit den sogenannten platonischen Körpern zu tun.

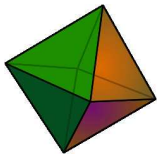
Bewegungen

Jede Symmetrie an einen Körper im Raum (beispielsweise einem Würfel) ist insbesondere eine abstandserhaltende, lineare Abbildung des umgebenden Raumes. Die Gesamtmenge der abstandserhaltenden, linearen (eigentlichen) Abbildungen des Raumes bildet die sogenannte *orthogonale Gruppe* O_3 (bzw. SO_3, wenn die Determinante 1 ist). Dies ist natürlich eine sehr große, unendliche Gruppe. Interessant ist aber, dass die endlichen Untergruppen darin übersichtlich beschrieben werden können. Diese endlichen Untergruppen lassen sich stets als Symmetriegruppe zu einem geeigneten geometrischen Objekt auffassen. Dass eine einfache Klassifikation dieser endlichen

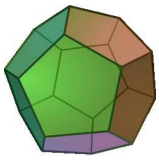
Bewegungsgruppen möglich ist, beruht auf intrinsischen Struktureigenschaften des Raumes und liefert unter Anderem eine präzise Version dafür, dass es nur fünf reguläre Polyder (die *platonischen Körper*) gibt.



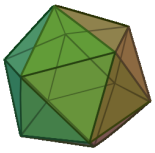
Ein Tetraeder (eine Pyramide mit gleichseitigen Dreiecken als Seiten).



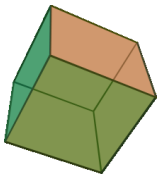
Ein Oktaeder (ein Achtflächner).



Ein Dodekaeder, der hat zwölf Seiten.



Ein Ikosaeder, mit 20 Seiten ...



... und ein Würfel. Das sind die platonischen Körper.

Für die folgenden Überlegungen benötigen wir etwas lineare Algebra, insbesondere den Begriff des euklidischen Vektorraumes und einer Isometrie.

Definition 21.1. Eine lineare Abbildung

$$\varphi\colon\ V \longrightarrow V$$

auf einem euklidischen Vektorraum V heißt *Isometrie*, wenn für alle $v, w \in V$ die Gleichheit

$$\langle \varphi(v), \varphi(w) \rangle \ = \ \langle v, w \rangle$$

gilt.

Definition 21.2. Eine Isometrie auf einem euklidischen Vektorraum heißt *eigentlich*, wenn ihre Determinante gleich 1 ist.

Die Gruppe, die aus allen Isometrien von V besteht, heißt *orthogonale Gruppe* zu V, und die eigentlichen Isometrien bilden die *spezielle orthogonale Gruppe*. Bei $V = \mathbb{R}^n$ schreibt man dafür

$$\mathrm{O}_n \ \text{ bzw. } \ \mathrm{SO}_n \ .$$

Eine eigentliche, lineare Isometrie nennt man auch eine *lineare Bewegung* (eine Spiegelung an einer Ebene im Raum ist also keine Bewegung). Unter einer *Bewegung* versteht man die „wirklich durchführbaren“ Transformationen des Raumes. Dazu gehören auch die Verschiebungen, die nur affin-linear, aber nicht linear sind.

Satz 21.3. *Sei V ein euklidischer Vektorraum und sei*

$$\varphi\colon\ V \longrightarrow V$$

eine lineare Isometrie. Dann besitzt jeder Eigenwert von φ den Betrag 1.

Beweis. Es sei $\varphi(v) = \lambda v$ mit $v \neq 0$, d.h. v ist ein Eigenvektor zum Eigenwert λ. Wegen der Isometrieeigenschaft gilt

$$||\, v \,|| = ||\, \varphi(v) \,|| = ||\, \lambda v \,|| = \ |\lambda| \cdot ||\, v \,|| \ .$$

Wegen $||\,v\,|| \neq 0$ folgt daraus $|\lambda| = 1$, also $\lambda = \pm 1$. □

Im Allgemeinen muss es keine Eigenwerte geben (bei ungerader Dimension allerdings schon).

Wir besprechen zunächst den zweidimensionalen Fall ausführlicher (im Eindimensionalen gibt es nur zwei lineare Isometrien: Die Identität und die Spiegelung $x \mapsto -x$).

Lineare Bewegungen in der Ebene

Satz 21.4. *Sei*

$$\varphi\colon\ \mathbb{R}^2 \longrightarrow \mathbb{R}^2$$

eine eigentliche, lineare Isometrie. Dann ist φ eine Drehung, und ihre Matrix hat die Gestalt

$$D(\theta) \;=\; \begin{pmatrix} \cos\,\theta & -\sin\,\theta \\ \sin\,\theta & \cos\,\theta \end{pmatrix}$$

mit einem eindeutig bestimmten Drehwinkel $\theta \in [0, 2\pi)$.

Beweis. Es seien (x, y) und (u, v) die Bilder der Einheitsvektoren $(1, 0)$ und $(0, 1)$. Unter einer Isometrie wird die Länge eines Vektors erhalten, daher ist

$$||\begin{pmatrix} x \\ y \end{pmatrix}|| = \sqrt{x^2 + y^2} \;=\; 1.$$

Daher ist x eine reelle Zahl zwischen -1 und $+1$ und $y = \pm\sqrt{1 - x^2}$, d.h. (x, y) ist ein Punkt auf dem reellen Einheitskreis. Der Einheitskreis wird bekanntlich durch die trigonometrischen Funktionen parametrisiert, d.h. es gibt einen eindeutig bestimmten Winkel θ, $0 \leq \theta < 2\pi$, mit

$$(x, y) = (\cos\,\theta, \sin\,\theta)\,.$$

Da unter einer Isometrie die Senkrechtsbeziehung erhalten bleibt, muss

$$\left\langle \begin{pmatrix} x \\ y \end{pmatrix}, \begin{pmatrix} u \\ v \end{pmatrix} \right\rangle \;=\; xu + yv \;=\; 0$$

gelten. Bei $y = 0$ folgt daraus (wegen $x = \pm 1$) $u = 0$. Dann ist $v = \pm 1$ und wegen der Eigentlichkeit muss das Vorzeichen dasselbe wie von x sein. Sei also $y \neq 0$. Dann gilt

$$\begin{pmatrix} -v \\ u \end{pmatrix} = \frac{u}{y} \begin{pmatrix} x \\ y \end{pmatrix}\,.$$

Da die zwei Vektoren die Länge 1 haben, muss der skalare Faktor u/y den Betrag 1 haben. Bei $u = y$ wäre $v = -x$ und die Determinante wäre -1. Also muss $u = -y \;\text{ und }\; v = x$ sein, was die Behauptung ergibt. □

Satz 21.5. *Sei $G \subseteq \mathrm{SO}_2$ eine endliche Untergruppe der linearen Bewegungsgruppe der reellen Ebene. Dann ist G eine zyklische Gruppe.*

Beweis. Jedes Element aus G ist nach Satz 21.4 eine Drehung der Ebene um einen bestimmten Winkel θ. Wir betrachten den surjektiven Gruppenhomomorphismus

$$\mathbb{R} \longrightarrow \mathrm{SO}_2,\ \theta \longmapsto D(\theta),$$

der einen Winkel auf die zugehörige Drehung abbildet. Es sei $H \subseteq \mathbb{R}$ das Urbild von G unter dieser Abbildung, d.h. H besteht aus allen Drehwinkeln zu Drehungen, die zu G gehören. Die Gruppe H wird von einem Repräsentantensystem für die Elemente aus G zusammen mit 2π erzeugt. Insbesondere ist also H eine endlich erzeugte Untergruppe von $\mathbb{R}$. Da jedes Gruppenelement aus G eine endliche Ordnung besitzt, muss jedes $\theta \in H$ die Gestalt $\theta = 2\pi q$ mit einer rationalen Zahl $q \in \mathbb{Q}$ haben. Dies bedeutet, dass H eine endlich erzeugte Untergruppe von $2\pi\mathbb{Q} \subseteq \mathbb{R}$ ist. Damit ist H isomorph zu einer endlich erzeugten Untergruppe der rationalen Zahlen. Nach Aufgabe 21.13 ist H zyklisch, sagen wir $H = \mathbb{Z}\alpha$ mit einem eindeutig bestimmten Winkel $\alpha \in [0, 2\pi)$. Dann ist die Gruppe G als Bild von H ebenfalls zyklisch. □

Wenn man auch noch uneigentliche Symmetrien, also Isometrien mit der Determinante -1 (etwa Achsenspiegelungen) zulässt, so gibt es noch eine weitere Familie von endlichen Untergruppen der O_2, nämlich die Diedergruppen.

Definition 21.6. Zu einem regelmäßigen n-Eck ($n \geq 2$) heißt die Gruppe der (eigentlichen oder uneigentlichen) linearen Symmetrien die *Diedergruppe* D_n.

Die Diedergruppe besteht aus den Drehungen des n-Ecks und aus den Achsenspiegelungen an den folgenden Achsen durch den Nullpunkt: bei n gerade die Achsen durch gegenüberliegende Eckpunkte und gegenüberliegende Kantenmittelpunkte, bei n ungerade die Achsen durch einen Eckpunkt und einen gegenüberliegenden Kantenmittelpunkt. In beiden Fällen besteht die Diedergruppe aus $2n$ Elementen.

Lineare Bewegungen im Raum

Satz 21.7. *Sei*

$$\varphi\colon\ \mathbb{R}^3 \longrightarrow \mathbb{R}^3$$

eine lineare Isometrie. Dann gibt es einen Eigenvektor zum Eigenwert 1 *oder* -1.

Beweis. Das charakteristische Polynom P zu φ ist ein normiertes Polynom vom Grad drei. Für $t \to +\infty$ geht $P(t) \to +\infty$ und für $t \to -\infty$ geht $P(t) \to -\infty$. Nach dem Zwischenwertsatz besitzt daher P mindestens eine Nullstelle. Eine solche Nullstelle ist ein Eigenwert von φ. Nach Satz 21.3 ist der Eigenwert gleich 1 oder gleich -1. □

Eine eigentliche lineare Isometrie des Raumes führt insbesondere die Einheitskugel durch eine Bewegung in sich über. Man kann sich eine solche Isometrie also gut als eine Drehung an einer Kugel vorstellen, die in einer passenden Schale liegt.

Satz 21.8. *Eine eigentliche Isometrie*

$$\varphi\colon \mathbb{R}^3 \longrightarrow \mathbb{R}^3$$

besitzt einen Eigenvektor zum Eigenwert 1*, d.h. es gibt eine Gerade (durch den Nullpunkt), die unter* φ *fest bleibt.*

Beweis. Wir betrachten das charakteristische Polynom von φ, also

$$P(\lambda) = \det(\lambda E_3 - \varphi).$$

Dies ist ein normiertes reelles Polynom vom Grad drei. Für $\lambda = 0$ ergibt sich

$$P(0) = \det(-\varphi) = -\det(\varphi) = -1.$$

Da für $\lambda \to \infty$ das Polynom $P(\lambda) \to \infty$ geht, muss es für ein positives λ eine Nullstelle geben. Aufgrund von Satz 21.3 kommt dafür nur $\lambda = 1$ in Frage. □

Lemma 21.9. *Sei*

$$\varphi\colon V \longrightarrow V$$

eine lineare Isometrie auf einem euklidischen Vektorraum V *und sei* $U \subseteq V$ *ein invarianter Unterraum. Dann ist auch das orthogonale Komplement* $U^\perp$ *invariant. Insbesondere kann man* φ *als direkte Summe*

$$\varphi = \varphi_U \oplus \varphi_{U^\perp}$$

schreiben, wobei die Einschränkungen φ_U *und* $\varphi_{U^\perp}$ *ebenfalls Isometrien sind.*

Beweis. Es ist

$$U^\perp = \{v \in V \mid \langle v, u\rangle = 0 \text{ für alle } u \in U\}.$$

Für ein solches $v \in U^\perp$ und ein beliebiges $u \in U$ ist

$$\langle \varphi(v), u\rangle = \langle \varphi^{-1}(\varphi(v)), \varphi^{-1}(u)\rangle = \langle v, u'\rangle = 0,$$

da $u' = \varphi^{-1}(u) \in U$ liegt wegen der Invarianz von U. Also ist wieder $\varphi(v) \in U^\perp$. □

Satz 21.10. *Sei*

$$\varphi\colon \mathbb{R}^3 \longrightarrow \mathbb{R}^3$$

eine eigentliche Isometrie. Dann ist φ *eine Drehung um eine feste Achse. Das bedeutet, dass* φ *in einer geeigneten Orthonormalbasis durch eine Matrix der Form*

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\alpha & -\sin\alpha \\ 0 & \sin\alpha & \cos\alpha \end{pmatrix}$$

beschrieben wird.

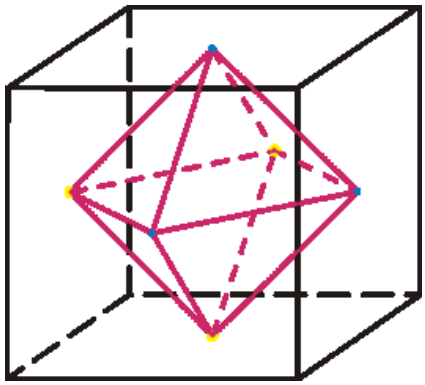
Beweis. Nach Satz 21.8 gibt es einen Eigenvektor u zum Eigenwert 1. Sei $U = \mathbb{R}u$ die davon erzeugte Gerade. Diese ist fix und insbesondere invariant unter φ. Nach Lemma 21.9 ist dann auch das orthogonale Komplement $U^\perp$ invariant unter φ, d.h. es gibt eine lineare Isometrie

$$\varphi_2 : U^\perp \longrightarrow U^\perp ,$$

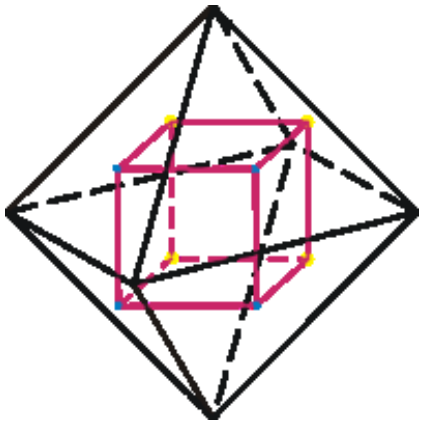
die auf $U^\perp$ mit φ übereinstimmt. Dabei muss φ_2 eigentlich sein, und daher muss nach Satz 21.4 φ_2 eine Drehung sein. Wählt man einen Vektor der Länge eins aus U und dazu eine Orthonormalbasis von $U^\perp$, so hat φ bzgl. dieser Basis die angegebene Gestalt. □

Halbachsensysteme

Es sei $G \subseteq \mathrm{SO}_3$ eine endliche Untergruppe der Gruppe der eigentlichen, linearen Isometrien. Jedes Element $g \in G$, $g \neq \mathrm{id}$, ist eine Drehung um eine eindeutig bestimmte Drehachse A. Insbesondere sind an einer endlichen Symmetriegruppe nur endlich viele Drehachsen beteiligt. Jedes Gruppenelement bewirkt dann eine Permutation der Drehachsenmenge, und diese Bedingung schränkt die möglichen Gruppen wesentlich ein. Eine Drehachse zerfällt in zwei Halbachsen, und es ist sinnvoll, die Wirkungsweise der Gruppe auf diesen Halbachsen zu untersuchen.



Würfel und Oktaeder besitzen



isomorphe Symmetriegruppen.

Bei einem Würfel gibt es drei verschiedene Arten von Drehachsen: Es gibt drei Drehachsen, die durch die Seitenmittelpunkte gegeben sind, vier Drehachsen, die durch die Eckpunkte gegeben sind und sechs Drehachsen, die durch die Kantenmittelpunkte gegeben sind. Betrachtet man alle *Durchstoßungspunkte* dieser Achsen mit der Sphäre vom Radius eins, so ergeben sich $6 + 8 + 12 = 26$ Punkte. Diese Punkte entsprechen den *Halbachsen*. Dabei gibt es zu je zwei Eckpunkten (bzw. den zugehörigen Durchstoßungspunkten) (mindestens) eine Würfelbewegung, die sie ineinander überführt, ebenso zu je zwei Kantenmittelpunkten und zu je zwei Seitenmittelpunkten. Jede Bewegung permutiert diese charakteristischen Punkte. Wenn man eine Achse (oder einen Durchstoßungspunkt) fixiert, so kann man die Menge der Bewegungen betrachten, die diese Achse als Drehachse haben. Es kann natürlich auch die Achse zwar auf sich selbst abgebildet werden, aber nicht fix sein. Dann werden die gegenüberliegenden Durchstoßungspunkte ineinander überführt.

Definition 21.11. Es sei $G \subseteq \mathrm{SO}_3(\mathbb{R})$ eine endliche Untergruppe der Gruppe der eigentlichen, linearen Isometrien im $\mathbb{R}^3$. Dann nennt man jede Gerade durch den Nullpunkt, die als Drehachse eines Elementes $g \neq \mathrm{id}$ auftritt, eine *Achse* von G. Die Halbgeraden dieser Drehachsen nennt man die *Halbachsen* der Gruppe und die Gesamtmenge dieser Halbachsen nennen wir das zu G gehörige *Halbachsensystem*. Es wird mit $\mathfrak{H}(G)$ bezeichnet. Zwei Halbachsen $H_1, H_2 \in \mathfrak{H}(G)$ heißen *äquivalent*, wenn es ein $g \in G$ gibt mit $g(H_1) = H_2$. Die Äquivalenzklassen zu dieser Äquivalenzrelation nennt man *Halbachsenklassen*.

Da jede von id verschiedene Drehung genau eine Drehachse hat, ist das Halbachsensystem zu einer endlichen Symmetriegruppe endlich (und zwar ist die Anzahl maximal gleich $2(\mathrm{ord}\,(G) - 1)$). Es liegt eine Gruppenoperation von G auf $\mathfrak{H}(G)$ durch $gH = g(H)$ vor. Die in obigen Definition erwähnten Äquivalenzklassen sind die Bahnen dieser Operation.

Beispiel 21.12. Beim Würfel werden die Halbachsen durch die Eckpunkte, die Seitenmittelpunkte und die Kantenmittelpunkte repräsentiert. Diese drei

Arten bilden dann auch die Äquivalenzklassen, also die Halbachsenklassen. Der Vergleich mit dem Oktaeder zeigt, dass die Sprechweise mit den Halbachsen für die Bewegungsgruppe als solche angemessener ist als die Sprechweise mit Ecken, Kanten, Mittelpunkten.

Beispiel 21.13. Bei einem Tetraeder gibt es vier Eck-Seitenmittelpunkt-Achsen und vier Kantenmittelpunktachsen. Die Kantenmittelpunkthalbachsen sind dabei alle untereinander äquivalent, während die zuerst genannten Achsen in zwei Halbachsenklassen zerfallen, nämlich die Eckhalbachsen und die Seitenhalbachsen.

An diesem Beispiel sieht man auch, dass die beiden durch eine Drehachse gegebenen Halbachsen nicht zueinander äquivalent sein müssen.

21. Arbeitsblatt

Aufwärmaufgaben

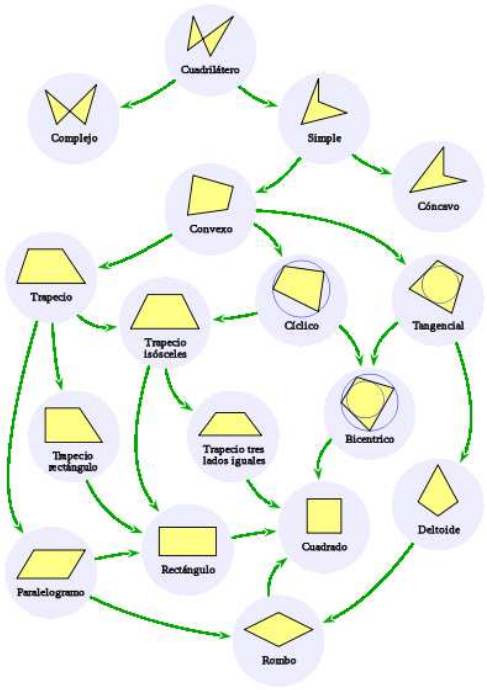
Aufgabe 21.1. Bestimme die Ordnung der ebenen Drehung um 291 Grad.

Die nächste Aufgabe verwendet die sogenannte *Kleinsche Vierergruppe*. Dies ist einfach die Produktgruppe $\mathbb{Z}/(2) \times \mathbb{Z}/(2)$.

Aufgabe 21.2. Zeige, dass die Diedergruppe D_2 isomorph zur Kleinschen Vierergruppe ist.

Aufgabe 21.3. Zeige, dass die Diedergruppe D_3 isomorph zur Permutationsgruppe S_3 ist.

Aufgabe 21.4. Es sei $V = (P_1, P_2, P_3, P_4)$ ein Viereck in der Ebene. Bestimme die möglichen eigentlichen Symmetriegruppen von V.



Aufgabe 21.5. Es sei $V = (P_1, P_2, P_3, P_4)$ ein Viereck in der Ebene. Bestimme die möglichen Symmetriegruppen (die auch die uneigentlichen Symmetrien beinhalten) von V.

Aufgabe 21.6. In die Erdkugel soll ein Würfel eingeschrieben werden derart, dass Osnabrück ein Eckpunkt ist und sich ein weiterer benachbarter Eckpunkt in südlicher Richtung von Osnabrück befindet. Bestimme die Koordinaten der Eckpunkte dieses Würfels. Wie viele Eckpunkte befinden sich im Meer?

Aufgabe 21.7. Führe folgendes Gedankenexperiment durch: Gegeben sei eine Kugeloberfläche aus Metall und n gleiche Teilchen mit der gleichen positiven Ladung. Die Teilchen stoßen sich also ab. Diese Teilchen werden auf die Kugeloberfläche gebracht, wobei sie sich nach wie vor gegenseitig abstoßen, aber auf der Kugel bleiben. Welche Konfiguration nehmen die Teilchen ein? Müsste sich nicht „aus physikalischen Gründen“ eine „gleichverteilte“ Konfiguration ergeben, in der alle Teilchen gleichberechtigt sind? Müsste es nicht zu je zwei Teilchen P, Q eine Kugelbewegung geben, die eine Symmetrie der Konfiguration ist und die P in Q überführt?

Aufgabe 21.8. Sei A_n eine alternierende Gruppe mit $n \geq 4$. Zeige, dass A_n nicht kommutativ ist.

Aufgabe 21.9. Zeige, dass die Kleinsche Vierergruppe zu einer Untergruppe der Permutationsgruppe S_4 isomorph ist. Wie sieht eine Realisierung als Untergruppe der Würfelgruppe aus?

Aufgabe 21.10. Zeige, dass jede gerade Permutation $\sigma \in S_n$, $n \geq 3$, ein Produkt aus Dreierzykeln ist.

Aufgabe 21.11. Betrachte die Wirkung der Tetraedergruppe auf den vier Eckpunkten eines Tetraeders. Zeige, dass dies eine Isomorphie zwischen der Tetraedergruppe und der alternierenden Gruppe A_4 ergibt.

Aufgabe 21.12. Sei $G \subseteq \mathrm{O}_2$ eine endliche Untergruppe der (eigentlichen und uneigentlichen) Bewegungsgruppe der reellen Ebene, und sei $G \not\subseteq \mathrm{SO}_2$. Zeige, dass es einen surjektiven Gruppenhomomorphismus

$$G \longrightarrow \mathbb{Z}/(2)$$

gibt, dessen Kern eine zyklische Gruppe ist. Schließe, dass die Ordnung von G gerade ist.

Aufgabe 21.13. Betrachte die rationalen Zahlen $(\mathbb{Q}, +, 0)$ als kommutative Gruppe. Es sei $G \subseteq \mathbb{Q}$ eine endlich erzeugte Untergruppe. Zeige, dass G zyklisch ist.

Aufgaben zum Abgeben

Aufgabe 21.14. (2 Punkte)

Wie viele Elemente besitzt die von der Drehung um 51 Grad, von der Drehung um 99 Grad und von der Siebteldrehung erzeugte Untergruppe der Drehgruppe SO_2?

Aufgabe 21.15. (3 Punkte)

Betrachte ein regelmäßiges n-Eck und die zugehörige Gruppe der (eigentlichen und uneigentlichen) Symmetrien, also die Diedergruppe D_n. Beschreibe D_n als Untergruppe der Permutationsgruppe S_n. Durch welche Permutationen wird sie erzeugt? Für welche n handelt es sich um eine Untergruppe der alternierenden Gruppe?

Die folgende Aufgabe verwendet den topologischen Begriff der Dichtheit.

Eine Teilmenge $T \subseteq \mathbb{R}$ heißt *dicht*, wenn es zu jeder reellen Zahl $x \in \mathbb{R}$ und jedem $\epsilon > 0$ Elemente $t \in T$ gibt mit $d(t,x) < \epsilon$.

Aufgabe 21.16. (3 Punkte)

Sei H eine (additive) Untergruppe der reellen Zahlen $\mathbb{R}$. Zeige, dass entweder $H = \mathbb{Z}a$ mit einer eindeutig bestimmten nicht-negativen reellen Zahl a ist, oder aber H dicht in $\mathbb{R}$ ist.

Aufgabe zum Hochladen

Aufgabe 21.17. (10 Punkte)

Schreibe eine Computeranimation, die zeigt, wie sich fünf auf einer Kugeloberfläche platzierte Teilchen mit der gleichen positiven Ladung aufgrund ihrer gegenseitigen Abstoßung bewegen (wobei sie aber auf der Kugeloberfläche bleiben), und welche Endposition (?) sie einnehmen.

22. Vorlesung - Symmetriegruppen II

Numerische Bedingungen für endliche Symmetriegruppen im Raum

Lemma 22.1. *Es sei $G \subseteq \mathrm{SO}_3(\mathbb{R})$ eine endliche Untergruppe der Gruppe der eigentlichen, linearen Isometrien des $\mathbb{R}^3$. Dann gelten folgende Aussagen.*

(1) *Für zwei äquivalente Halbachsen H_1 und H_2 sind die Isotropiegruppen $G_{H_1} = \{g \in G | \, g(H_1) = H_1\}$ und $G_{H_2} = \{g \in G | \, g(H_2) = H_2\}$ isomorph.*

(2) *Zu einer Halbachse H aus der Halbachsenklasse K ist*

$$\#(G) = \#(K) \cdot \#(G_H).$$

(3) *Zu einer Halbachsenklasse K ist die Abbildung*

$$G \longrightarrow \mathrm{Perm}(K),\, g \longmapsto (\sigma_g : H \mapsto g(H)),$$

ein Gruppenhomomorphismus, dessen Kern die Isotropiegruppe ist.

(4) *Die Isotropiegruppen zu einer Halbachse H und der gegenüberliegenden Halbachse $-H$ sind isomorph.*

Beweis. (1), (2), (3) folgen aus allgemeinen Eigenschaften von Gruppenoperationen, angewendet auf die natürliche Operation von G auf dem Halbachsensystem $\mathfrak{H}(G)$. (4) folgt daraus, dass eine Drehung, die H in sich überführt, eine Drehung um die durch H festgelegte Achse ist und daher auch die andere Achsenhälfte in sich überführt. □

Die Isotropiegruppe G_H besteht aus Drehungen um eine Achse und ist daher nach Satz 21.5 eine zyklische Gruppe. Die Ordnung der Gruppe nennt man auch die *Drehordnung* der Achse.

Lemma 22.2. *Es sei $G \subseteq \mathrm{SO}_3(\mathbb{R})$ eine endliche Untergruppe der Ordnung n in der Gruppe der eigentlichen, linearen Isometrien des $\mathbb{R}^3$. Es seien $K_1, \ldots, K_m$ die verschiedenen Halbachsenklassen zu G, und zu jeder dieser Klassen sei n_i, $i = 1, \ldots, m$, die Ordnung der Gruppe G_H, $H \in K_i$, die nach Lemma 22.1 unabhängig von $H \in K_i$ ist. Dann ist*

$$2\left(1 - \frac{1}{n}\right) = \sum_{i=1}^{m} \left(1 - \frac{1}{n_i}\right)$$

Beweis. Für zwei gegenüberliegende Halbachsen H und $-H$ gilt $G_H = G_{-H}$. Dagegen gilt für zwei Halbachsen H_1 und H_2, die nicht zur gleichen Achse gehören (also insbesondere verschieden sind), die Beziehung $G_{H_1} \cap G_{H_2} = \{\mathrm{id}\}$, da eine Isometrie mit zwei Fixachsen die Identität sein muss. Da G die Vereinigung aller G_H, $H \in \mathfrak{H}(G)$, ist, liegt eine Vereinigung

$$G \setminus \{\mathrm{id}\} = \bigcup_{H \in \mathfrak{H}(G)} (G_H \setminus \{\mathrm{id}\})$$

vor, wobei rechts jedes Gruppenelement $g \neq \mathrm{id}$ genau zweimal vorkommt. Daher ist

$$2(n-1) \;=\; \sum_{H \in \mathfrak{H}(G)} (\mathrm{ord}\,(G_H) - 1)\,.$$

Die Halbachsenklasse K_i enthält n/n_i Elemente. Daher ist

$$2(n-1) \;=\; \sum_{H \in \mathfrak{H}(G)} (\mathrm{ord}\,(G_H) - 1) \;=\; \sum_{i=1}^{m} \frac{n}{n_i}(n_i - 1).$$

Mittels Division durch n ergibt sich die Behauptung. □

Lemma 22.3. *Die numerische Gleichung*

$$2\left(1 - \frac{1}{n}\right) = \sum_{i=1}^{m} \left(1 - \frac{1}{n_i}\right)$$

mit $n \geq 2$, $m \in \mathbb{N}$ und mit $2 \leq n_1 \leq n_2 \leq \ldots \leq n_m$ besitzt folgende Lösungen.

(1) *$m = 2$ und $n = n_1 = n_2$.*
(2) *Bei $m = 3$ gibt es die Möglichkeiten*
   (a) *$n_1 = n_2 = 2$ und $n = 2n_3$,*
   (b) *$n_1 = 2$, $n_2 = n_3 = 3$ und $n = 12$,*
   (c) *$n_1 = 2$, $n_2 = 3$, $n_3 = 4$ und $n = 24$,*
   (d) *$n_1 = 2$, $n_2 = 3$, $n_3 = 5$ und $n = 60$.*

Beweis. Bei $m = 0$ ist die rechte Seite 0 und daher folgt $n = 1 < 2$ aus der linken Seite. Bei $m = 1$ muss $n_1 = \frac{n}{-n+2}$ gelten, was bei $n \geq 2$ keine Lösung besitzt. Bei $m = 2$ erhält man die Bedingung

$$\frac{2}{n} = \frac{1}{n_1} + \frac{1}{n_2},$$

woraus sich $n_1 = n_2 = n$ ergibt. Bei $m = 3$ schreibt sich die Bedingung als

$$1 + \frac{2}{n} = \frac{1}{n_1} + \frac{1}{n_2} + \frac{1}{n_3}$$

mit $n_1 \leq n_2 \leq n_3$. Die linke Seite ist > 1. Daher muss wegen $n_i \geq 2$ mindestens eines der $n_i = 2$ sein. Sei also $n_1 = 2$. Bei $n_2 = 2$ gibt es genau die Lösung $n = 2n_3$ mit beliebigem $n_3 \geq 2$. Sei also $n_2 \geq 3$. Bei $n_2 \geq 4$ wäre die rechte Seite wieder ≤ 1, so dass $n_2 = 3$ gelten muss. Der Wert $n_3 = 3$ führt zur Lösung $n = 12$, der Wert $n_3 = 4$ führt zur Lösung $n = 24$ und der Wert $n_3 = 5$ führt zur Lösung $n = 60$. Bei $n_3 \geq 6$ wird die rechte Seite wieder ≤ 1, so dass es keine weitere Lösung gibt. Bei $m \geq 4$ hat man eine Bedingung der Form

$$m - 2 + \frac{2}{n} = \frac{1}{n_1} + \frac{1}{n_2} + \frac{1}{n_3} + \frac{1}{n_4} + \ldots + \frac{1}{n_m},$$

die keine Lösung besitzt, da die rechte Seite $\leq m - 2$ ist, da die ersten vier Summanden maximal 2 ergeben und die weiteren durch $m - 4$ abgeschätzt werden können. □

Bei $m \geq 3$ nennen wir (n_1, n_2, n_3) den *numerischen Typ* der Untergruppe G.

Geometrische Realisierungen der endlichen Symmetriegruppen

Das letzte Lemma enthält die entscheidenden numerischen Bedingungen, wie eine endliche Symmetriegruppe im $\mathbb{R}^3$ aussehen kann. Wenn man von der trivialen Gruppe absieht, bei der $m = 0$ gilt, so erfasst dieses Lemma alle endlichen Gruppen, da bei $m \geq 1$ für jedes i die Gruppe der Drehungen an einer Achse schon mindestens zwei Elemente besitzt, also $n_i \geq 2$ ist. Jede der angegebenen Bedingungen lässt sich im Wesentlichen eindeutig durch eine endliche Symmetriegruppe realisieren. Das geometrische Objekt ist aber nicht eindeutig bestimmt, wie schon das „duale Paar“ Würfel und Oktaeder zeigen.

Plato (427-347 v. C.) sagte: „die Bedeutung der Geometrie beruht nicht auf ihrem praktischen Nutzen, sondern darauf, daß sie ewige und unwandelbare Gegenstände untersucht und danach strebt, die Seele zur Wahrheit zu erheben“.

Lemma 22.4. *Es sei $G \subseteq \mathrm{SO}_3(\mathbb{R})$ eine endliche Untergruppe der Ordnung n der Gruppe der eigentlichen linearen Isometrien des $\mathbb{R}^3$ mit zwei verschiedenen Halbachsenklassen zu G. Dann ist G die zyklische Gruppe der Drehungen zum Winkel $2\pi/n$ um eine einzige fixierte Drehachse.*

Beweis. Aufgrund von Lemma 22.2 und Lemma 23.2 muss $n = n_1 = n_2$ sein und jede Halbachsenklasse enthält nur eine Halbachse. Daher gibt es überhaupt nur eine Drehachse und diese Bewegungsgruppe ist isomorph zu einer Bewegungsgruppe in der senkrechten Ebene, also nach Satz 21.5 isomorph zur zyklischen Gruppe der Ordnung n. □

In diesem Fall gibt es also zwei Halbachsenklassen, die jeweils aus nur einer Halbachse bestehen.

Lemma 22.5. *Es sei $G \subseteq \mathrm{SO}_3(\mathbb{R})$ eine endliche Untergruppe der Gruppe der eigentlichen, linearen Isometrien des $\mathbb{R}^3$ vom Typ $(2, 2, k)$. Dann ist G isomorph zur Diedergruppe D_k.*

Beweis. Es gibt drei Halbachsenklassen, und zwar zwei mit der Ordnung 2 (und je k Halbachsen in der Klasse) und eine mit der Ordnung k und zwei Halbachsen (die Anzahlen der Halbachsen folgen mit $n_1 = n_2 = 2$ aus Lemma 23.2). Bei $k \geq 3$ müssen die zwei Halbachsen aus der dritten Klasse eine Gerade bilden, da ja die gegenüberliegende Halbachse die gleiche Ordnung besitzt, und bei $k = 2$ muss jede Halbachse zu ihrem Gegenüber äquivalent sein. Wir bezeichnen die Achse zu K_3 mit A_3. Jedes Gruppenelement mit einer anderen Drehachse muss die beiden Halbachsen aus K_3 ineinander überführen, so dass alle anderen Achsen senkrecht zu A_3 stehen. Es sei g eine

erzeugende Drehung um A_3. Zu einer Halbachse H_1 aus K_1 sind die

$$g^i(H_1), i = 0, \ldots, k-1,$$

genau alle Halbachsen aus K_1. Diese bilden ein regelmäßiges k-Eck in der zu A_3 senkrechten Ebene. Entsprechendes gilt für $g^i(H_2)$ mit $H_2 \in K_2$. Jede Halbdrehung um eine der Achsen aus K_1 überführt die Halbachsen aus K_2 in ebensolche. Daher liefern die Halbachsen aus K_2 eine „Halbierung“ des k-Ecks. Somit handelt es sich insgesamt um die (uneigentliche) Symmetriegruppe eines regelmäßigen k-Ecks, d.h. um eine Diedergruppe D_k. □

In diesem Fall bestehen die beiden Halbachsenklassen der Ordnung zwei einerseits aus den Eckpunkten (oder Eckhalbachsen) und andererseits aus den Seitenmittelpunkten (oder Seitenmittelhalbachsen) des zugrunde liegenden regelmäßigen $n/2$-Ecks. Bei $n/2$ gerade sind gegenüberliegende Halbachsen äquivalent, bei $n/2$ ungerade nicht. Bei $n = 4$ ist die Diedergruppe (also D_2) kommutativ und isomorph zur Kleinschen Vierergruppe.

Lemma 22.6. *Es sei $G \subseteq \mathrm{SO}_3(\mathbb{R})$ eine endliche Untergruppe der Gruppe der eigentlichen, linearen Isometrien des $\mathbb{R}^3$ vom Typ $(2,3,3)$. Dann ist G die Tetraedergruppe und damit isomorph zur alternierenden Gruppe A_4.*

Beweis. Nach Voraussetzung gibt es drei Halbachsenklassen der Ordnung $2, 3$ und 3, ihre Elementanzahl ist daher $6, 4$ und 4. Betrachten wir eine Halbachsenklasse K der Ordnung 3 mit ihren vier äquivalenten Halbachsen und den zugehörigen Gruppenhomomorphismus

$$G \longrightarrow \mathrm{Perm}\,(K),\ g \longmapsto \sigma_g.$$

Sei $g \in G$ eine Dritteldrehung um eine Halbachse $H \in K$. Sie lässt H fest und bewirkt eine Permutation der drei anderen Halbachsen in der Klasse. Diese Permutation kann nicht die Identität sein, da sonst g mindestens zwei Achsen fest ließe und damit g die (Raum)-Identität wäre. Da g die Ordnung 3 besitzt, muss diese Permutation ein Dreierzykel sein. Insbesondere gehören die vier Halbachsen zu verschiedenen Achsen, und die Doppeldrehung g^2 bewirkt den anderen Dreierzykel. Da man diese Überlegung mit jeder der vier Halbachsen anstellen kann, sieht man, dass G sämtliche Dreierzykel der Permutationsgruppe der vier Halbachsen bewirkt. Das Bild des Gruppenhomomorphismus ist daher genau die alternierende Gruppe A_4 und damit ist $G \cong A_4$. Diese ist nach Aufgabe 21.11 isomorph zur Tetraedergruppe. □

In der vorstehenden Aussage kann man auch direkt erkennen, dass es sich um eine Tetradergruppe handeln muss. Dazu markieren wir auf jeder der vier Halbachsen den Punkt mit dem Abstand 1 zum Nullpunkt. Aus dem Beweis des Lemmas folgt, dass je zwei solche Punkte den gleichen Abstand voneinander haben (und dass die Winkel der Halbachsen zueinander alle gleich sind). Daher bilden diese vier Punkte die Eckpunkte eines Tetraeders. Die

gegenüberliegenden Halbachsen entsprechen den Seitenmittelpunkten der Tetraederflächen. Das Halbachsensystem der Ordnung zwei wird gebildet durch die Kantenmittelpunkte.

Lemma 22.7. *Es sei $G \subseteq \mathrm{SO}_3(\mathbb{R})$ eine endliche Untergruppe der Gruppe der eigentlichen, linearen Isometrien des $\mathbb{R}^3$ vom Typ $(2,3,4)$. Dann ist G isomorph zur Permutationsgruppe S_4 und konjugiert zur Würfelgruppe.*

Beweis. Wir betrachten die Halbachsenklasse K_2 der Ordnung 3, die also 8 zueinander äquivalente Halbachsen besitzt. Zu einer solchen Halbachse H muss die entgegengesetzte Halbachse ebenfalls in einer der Halbachsenklassen liegen, und zwar in einer mit der gleichen Ordnung. Daher gehört auch $-H$ zu K_2, so dass an K_2 insgesamt vier Achsen beteiligt sind. Die Menge dieser Achsen nennen wir $\mathfrak{A}$. Wir betrachten den Gruppenhomomorphismus

$$G \longrightarrow \mathrm{Perm}(\mathfrak{A}),\ g \longmapsto (\sigma_g : A \mapsto g(A))\,.$$

Hier wird also nur geschaut, was mit den Achsen passiert, nicht was mit den Halbachsen. Es können nicht drei dieser vier Achsen in einer Ebene liegen. Wären nämlich $A_1, A_2, A_3 \subseteq E$, so würde eine Dritteldrehung f um A_1 die äquivalenten Achsen $f(A_2)$ und $f(A_3)$ hervorbringen, die aber nicht in der Ebene E liegen können und die nicht beide gleich A_4 sein können. Das Element $g \in G$ habe die Eigenschaft, dass σ_g die Identität ist, dass also alle Geraden $A \in \mathfrak{A}$ auf sich abgebildet werden. Nach Aufgabe 22.9 muss g die Identität sein. Der Gruppenhomomorphismus ist also nach dem Kernkriterium injektiv und daher muss eine Isomorphie vorliegen. □

Die vier Achsen in dem Beweis bilden die Raumdiagonalen eines Würfels. Man kann also jede Permutation der Raumdiagonalen (als Teilmengen; diese Diagonalen können also auch umgeklappt werden) in eindeutiger Weise als eine Würfelsymmetrie realisieren.

Mit einem ähnlichen, aber aufwändigeren Argument kann man zeigen, dass die verbleibende numerische Möglichkeit, also eine Gruppe mit 60 Elementen und mit den Drehordnungen $2, 3$ und 5 wieder nur von einem Isomorphietyp realisiert wird, nämlich von der alternierenden Gruppe A_5, die zugleich isomorph zur Dodekaedergruppe und zur Ikosaedergruppe ist.

Insgesamt haben wir (bis auf den Ikosaederfall) den folgenden Hauptsatz über endliche (eigentliche) Symmetriegruppen im Raum bewiesen.

Satz 22.8. *Es sei $G \subseteq \mathrm{SO}_3(\mathbb{R})$ eine endliche Untergruppe der Gruppe der eigentlichen, linearen Isometrien des $\mathbb{R}^3$. Dann ist G eine der folgenden Gruppen.*

(1) *Eine zyklische Gruppe $\mathbb{Z}/(n)$, $n \geq 1$,*
(2) *Eine Diedergruppe D_k, $k \geq 2$,*
(3) *Die Tetraedergruppe A_4,*
(4) *Die Würfelgruppe S_4,*

(5) *Die Ikosaedergruppe* A_5.

Wenn man die obigen Argumentationen etwas verfeinert, so erhält man, dass jede endliche Untergruppe zu den angegebenen Symmetriegruppen sogar konjugiert ist.

22. Arbeitsblatt

Aufwärmaufgaben

Aufgabe 22.1. Es liege eine Gruppenoperation einer Gruppe G auf einer Menge M vor. Zeige, dass die Isotropiegruppen zu zwei äquivalenten Elementen $x, y \in M$ in natürlicher Weise isomorph sind.

Aufgabe 22.2. Betrachte den Beweis zu Lemma 22.2 mit der dortigen Notation. Begründe die folgenden Aussagen.

(1) Eine eigentliche Isometrie mit zwei Fixachsen ist die Identität.
(2) G ist die Vereinigung aller G_H.
(3) Sei $g \neq \mathrm{id}$. Das Element g kommt in genau zwei der G_H vor. In welchen?
(4) Die Halbachsenklasse K_i enthält n/n_i Elemente.

Aufgabe 22.3. Überprüfe die Formel

$$2\left(1-\frac{1}{n}\right) = \sum_{i=1}^{m}\left(1-\frac{1}{n_i}\right)$$

für den Oktaeder, den Dodekaeder und den Ikosaeder.

Aufgabe 22.4. Sei G eine Gruppe, M eine Menge und

$$G \longrightarrow \mathrm{Perm}\,(M),\ g \longmapsto \sigma_g,$$

ein Gruppenhomomorphismus in die Permutationsgruppe von M. Zeige, dass dies in natürlicher Weise einen Gruppenhomomorphismus

$$G \longrightarrow \mathrm{Perm}(\mathfrak{P}\,(\mathrm{M}))\,,\ g \longmapsto (N \mapsto g(N)),$$

in die Permutationsgruppe der Potenzmenge induziert.

Aufgabe 22.5. Betrachte ein gleichseitiges Dreieck mit dem Nullpunkt als Mittelpunkt und mit $(1,0)$ als einem Eckpunkt. Bestimme die (eigentlichen und uneigentlichen) Matrizen, die den Symmetrien an diesem Dreieck entsprechen.

Aufgabe 22.6. Bestimme sämtliche Matrizen, die den Symmetrien eines Quadrates mit den Eckpunkten $(\pm 1, \pm 1)$ entsprechen. Sehen diese Matrizen für jedes Quadrat (mit dem Nullpunkt als Mittelpunkt) gleich aus?

Aufgabe 22.7. Zeige, dass sich jede endliche Gruppe als Untergruppe der $\mathrm{SO}_n(\mathbb{R})$ realisieren lässt.

Aufgabe 22.8. Man gebe ein Beispiel einer Raumdrehung, bei der sämtiche Matrixeinträge $\neq 0, 1$ sind.

Aufgaben zum Abgeben

Aufgabe 22.9. (4 Punkte)

Es seien A_1, A_2, A_3 und A_4 vier Geraden im $\mathbb{R}^3$ durch den Nullpunkt mit der Eigenschaft, dass keine drei davon in einer Ebene liegen. Es sei

$$f\colon \mathbb{R}^3 \longrightarrow \mathbb{R}^3$$

eine lineare, eigentliche Isometrie mit $f(A_i) = A_i$ für $i = 1, 2, 3, 4$. Zeige, dass f die Identität ist. Man gebe ein Beispiel an, dass diese Aussage ohne die Ebenenbedingung nicht gilt.

Aufgabe 22.10. (4 Punkte)

Es seien $\varphi_1, \varphi_2, \varphi_3$ Drehungen um die x-Achse, die y-Achse und die z-Achse mit den Ordungen n_1, n_2, n_3 (φ_1 ist also eine Drehung um den Winkel $360/n_1$ Grad um die x-Achse, etc.). Es sei $1 \leq n_1 \leq n_2 \leq n_3$. Für welche Tupel (n_1, n_2, n_3) ist die von diesen drei Drehungen erzeugte Gruppe endlich?

Aufgabe 22.11. (3 Punkte)

Zeige: Keine der alternierenden Gruppen A_n besitzt eine Untergruppe vom Index zwei.

23. Vorlesung - Ebene komplexe Gruppen I

In den folgenden Vorlesungen möchten wir die endlichen Untergruppen $G \subseteq \mathrm{SL}_2(\mathbb{C})$ (bis auf Konjugation) und die zugehörigen Invariantenringe $K[U,V]^G$ bestimmen. Es wird sich herausstellen, dass es hierzu eine überschaubare Klassifikation gibt, nämlich die ADE-Klassifikation. Die auftretenden Invariantenringe bzw. ihre Spektren (also die Bahnenräume) nennt man *ADE-Singularitäten*. Von Singularitäten spricht man, da diese Invariantenringe keine Polynomringe sind, also nicht „regulär“ sind. Die anvisierte Klassifikation beruht auf der Klassifikation der endlichen Bewegungsgruppen im $\mathbb{R}^3$.

Eine Liste von Untergruppen der $\mathrm{SL}_2(\mathbb{C})$

Wir betrachten die folgenden Beispiele von endlichen Untergruppen der $\mathrm{SL}_2(\mathbb{C})$. Wir werden später sehen, dass diese Liste bis auf Konjugation vollständig ist.

Beispiel 23.1. Die zyklische Gruppe der Ordnung n lässt sich einfach als eine Untergruppe der $\mathrm{SL}_2(\mathbb{C})$ realisieren. Dazu sei ζ eine n-te komplexe primitive Einheitswurzel, beispielsweise $\zeta = e^{\frac{2\pi i}{n}}$. Die von

$$\begin{pmatrix} \zeta & 0 \\ 0 & \zeta^{n-1} \end{pmatrix} = \begin{pmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{pmatrix}$$

erzeugte Untergruppe, also

$$\left\{ \begin{pmatrix} \zeta^j & 0 \\ 0 & \zeta^{-j} \end{pmatrix} \mid j = 0, \ldots, n-1 \right\} \subseteq \mathrm{SL}_2(\mathbb{C}) \ ,$$

ist eine zyklische Gruppe der Ordnung n. Diese Untergruppe wird mit Z_n bezeichnet.

Beispiel 23.2. Sei $n \in \mathbb{N}_+$ und sei ζ eine $2n$-te komplexe primitive Einheitswurzel, beispielsweise

$$\zeta \ = \ e^{\frac{2\pi i}{2n}} \ = \ e^{\frac{\pi i}{n}}.$$

Die von den Matrizen

$$A = A_{2n} = \begin{pmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{pmatrix} \text{ und } B = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

erzeugte Untergruppe der $\mathrm{SL}_2(\mathbb{C})$ heißt die *binäre Diedergruppe*. Sie wird mit BD_n bezeichnet. Das Element A besitzt die Ordnung $2n$ und es ist

$$A^n \ = \ \begin{pmatrix} \zeta^n & 0 \\ 0 & \zeta^{-n} \end{pmatrix} \ = \ \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \ = \ B^2.$$

Insbesondere besitzt B die Ordnung 4. Es ist

$$BA \ = \ \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \begin{pmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{pmatrix} \ = \ \begin{pmatrix} 0 & i\zeta^{-1} \\ i\zeta & 0 \end{pmatrix} \ = \ \begin{pmatrix} \zeta^{-1} & 0 \\ 0 & \zeta \end{pmatrix} \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \ = \ A^{2n-1}B.$$

Somit lassen sich alle Elemente der Gruppe als

$$A^iB^j \text{ mit } 0 \leq i \leq 2n-1,\ 0 \leq j \leq 1,$$

schreiben. Da B nicht zu der von A erzeugten Untergruppe gehört, ist diese Darstellung eindeutig und BD_n besitzt genau $4n$ Elemente. Es liegt die Untergruppenbeziehung $Z_{2n} \subseteq BD_n$ vom Index 2 vor.

Beispiel 23.3. Die Matrizen

$$A = A_8 = \begin{pmatrix} \zeta & 0 \\ 0 & \zeta^7 \end{pmatrix},\ B = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \text{ und } C = \frac{1}{\sqrt{2}} \begin{pmatrix} \zeta^7 & \zeta^7 \\ \zeta^5 & \zeta \end{pmatrix},$$

wobei ζ eine primitive achte Einheitswurzel ist, erzeugen eine Untergruppe von $\mathrm{SL}_2(\mathbb{C})$. Die Ordnungen dieser Elemente ergeben sich folgendermaßen. Es ist

$$A^4 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = B^2,$$

also besitzt A die Ordnung 8 und B die Ordnung 4. Mit

$$\zeta = e^{\frac{2\pi i}{8}} = e^{\frac{\pi i}{4}} = \frac{1+i}{\sqrt{2}}$$

ist

$$\begin{aligned} C^3 &= \frac{1}{2\sqrt{2}} \begin{pmatrix} \zeta^7 & \zeta^7 \\ \zeta^5 & \zeta \end{pmatrix} \begin{pmatrix} \zeta^7 & \zeta^7 \\ \zeta^5 & \zeta \end{pmatrix} \begin{pmatrix} \zeta^7 & \zeta^7 \\ \zeta^5 & \zeta \end{pmatrix} \\ &= \frac{1}{2\sqrt{2}} \begin{pmatrix} \zeta^6+\zeta^4 & \zeta^6+1 \\ \zeta^4+\zeta^6 & \zeta^4+\zeta^2 \end{pmatrix} \begin{pmatrix} \zeta^7 & \zeta^7 \\ \zeta^5 & \zeta \end{pmatrix} \\ &= \frac{1}{2\sqrt{2}} \begin{pmatrix} \zeta^5+\zeta^3+\zeta^3+\zeta^5 & \zeta^5+\zeta^3+\zeta^7+\zeta \\ \zeta^3+\zeta^5+\zeta+\zeta^7 & \zeta^3+\zeta^5+\zeta^5+\zeta^3 \end{pmatrix} \\ &= \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \end{aligned}$$

so dass die Ordnung von C gleich 6 ist. Jedes Element dieser Gruppe kann man als $A^iB^jC^k$ schreiben, wobei die Exponenten jeweils maximal bis zur Ordnung der Matrizen laufen. Um das einzusehen muss man untersuchen, was passiert, wenn man ein solches Element mit A oder B rechterhand multipliziert. Es ist

$$\begin{aligned} CA &= \frac{1}{\sqrt{2}} \begin{pmatrix} \zeta^7 & \zeta^7 \\ \zeta^5 & \zeta \end{pmatrix} \begin{pmatrix} \zeta & 0 \\ 0 & \zeta^7 \end{pmatrix} \\ &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & \zeta^6 \\ \zeta^6 & 1 \end{pmatrix} \\ &= \frac{1}{2} \begin{pmatrix} \sqrt{2} & -\sqrt{2}i \\ -\sqrt{2}i & \sqrt{2} \end{pmatrix} \\ &= \frac{1}{2} \begin{pmatrix} \zeta+\zeta^7 & \zeta^5+\zeta^7 \\ \zeta^7+\zeta^5 & \zeta^7+\zeta \end{pmatrix} \\ &= \frac{1}{2} \begin{pmatrix} \zeta & 0 \\ 0 & \zeta^7 \end{pmatrix} \begin{pmatrix} 1+\zeta^6 & \zeta^4+\zeta^6 \\ 1+\zeta^6 & 1+\zeta^2 \end{pmatrix} \end{aligned}$$

$$\begin{aligned} &= \frac{1}{2}\begin{pmatrix}\zeta & 0\\ 0 & \zeta^7\end{pmatrix}\begin{pmatrix}0 & i\\ i & 0\end{pmatrix}\begin{pmatrix}\zeta^6+\zeta^4 & \zeta^6+1\\ \zeta^4+\zeta^6 & \zeta^4+\zeta^2\end{pmatrix}\\ &= \frac{1}{2}\begin{pmatrix}\zeta & 0\\ 0 & \zeta^7\end{pmatrix}\begin{pmatrix}0 & i\\ i & 0\end{pmatrix}\begin{pmatrix}\zeta^7 & \zeta^7\\ \zeta^5 & \zeta\end{pmatrix}^2\\ &= ABC^2, \end{aligned}$$

man kann also A von rechts an C vorbeischieben. Wegen

$$\begin{aligned} CB &= \frac{1}{\sqrt{2}}\begin{pmatrix}\zeta^7 & \zeta^7\\ \zeta^5 & \zeta\end{pmatrix}\begin{pmatrix}0 & i\\ i & 0\end{pmatrix}\\ &= \frac{1}{\sqrt{2}}\begin{pmatrix}\zeta & \zeta\\ \zeta^3 & \zeta^7\end{pmatrix}\\ &= \frac{1}{\sqrt{2}}\begin{pmatrix}i & 0\\ 0 & -i\end{pmatrix}\begin{pmatrix}\zeta^7 & \zeta^7\\ \zeta^5 & \zeta\end{pmatrix}\\ &= A^2C \end{aligned}$$

kann man B von rechts an C vorbeischieben. Wegen

$$\begin{aligned} BA &= \begin{pmatrix}0 & i\\ i & 0\end{pmatrix}\begin{pmatrix}\zeta & 0\\ 0 & \zeta^7\end{pmatrix}\\ &= \begin{pmatrix}0 & \zeta\\ \zeta^3 & 0\end{pmatrix}\\ &= \begin{pmatrix}\zeta^7 & 0\\ 0 & \zeta\end{pmatrix}\begin{pmatrix}0 & i\\ i & 0\end{pmatrix}\\ &= \begin{pmatrix}\zeta & 0\\ 0 & \zeta^7\end{pmatrix}^7\begin{pmatrix}0 & i\\ i & 0\end{pmatrix}\\ &= A^7B \end{aligned}$$

kann man B von rechts an A vorbeischieben. Wegen

$$C^3 = \begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix} = A^4 = B^2$$

kann man sogar jedes Gruppenelement als

$$A^iB^jC^k \text{ mit } 0 \le i \le 7,\ 0 \le j \le 1,\ 0 \le k \le 2,$$

schreiben.

Wir zeigen, dass es unter diesen Elementen keine Wiederholungen gibt. Die Produkte A^iB^j mit $0 \le i \le 7$, $0 \le j \le 1$, bilden nach Beispiel 23.2 die binäre Diedergruppe BD_4 der Ordnung 16, dort gibt es also keine Wiederholungen. Also enthält die Gruppe eine Untergruppe der Ordnung 16 aber auch eine Untergruppe der Ordnung 3 (die von C^2 erzeugte Untergruppe), also muss ihre Ordnung 48 sein (und in den obigen Produkten kann es keine Wiederholung geben). Es handelt sich also um eine Gruppe mit 48 Elementen, die die *binäre Oktaedergruppe* heißt. Sie wird mit BO bezeichnet. Es liegt die Untergruppenbeziehung

$$Z_8 \subseteq BD_4 \subseteq BO$$

vor.

Beispiel 23.4. Es seien

$$A = \begin{pmatrix} \zeta & 0 \\ 0 & \zeta^7 \end{pmatrix},\ B = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \text{ und } C = \frac{1}{\sqrt{2}} \begin{pmatrix} \zeta^7 & \zeta^7 \\ \zeta^5 & \zeta \end{pmatrix},$$

wobei ζ eine primitive achte Einheitswurzel ist, die Erzeuger der binären Oktaedergruppe BO. Die darin von A^2, B, C erzeugte Untergruppe besteht aus allen Elementen $A^{2i}B^jC^k$ mit $0 \leq i \leq 3$, $0 \leq j \leq 1$, $0 \leq k \leq 2$, wie ähnliche Berechnungen wie die aus Beispiel 23.3 zeigen, und besitzt demnach 24 Elemente. Diese Gruppe nennt man die *binäre Tetraedergruppe*, sie wird mit BT bezeichnet.

Beispiel 23.5. Es sei ξ eine primitive 5-te komplexe Einheitswurzel. Wir setzen

$$E = -\begin{pmatrix} \xi^3 & 0 \\ 0 & \xi^2 \end{pmatrix} \text{ und } F = \frac{1}{\sqrt{5}} \begin{pmatrix} -\xi + \xi^4 & \xi^2 - \xi^3 \\ \xi^2 - \xi^3 & \xi - \xi^4 \end{pmatrix}.$$

Die von diesen Elementen erzeugte Untergruppe der $\mathrm{SL}_2(\mathbb{C})$ heißt die *binäre Ikosaedergruppe*. Es ist

$$E^5 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

und somit besitzt E die Ordnung 10. Wegen

$$\begin{aligned} F^2 &= \frac{1}{5} \begin{pmatrix} -\xi + \xi^4 & \xi^2 - \xi^3 \\ \xi^2 - \xi^3 & \xi - \xi^4 \end{pmatrix} \cdot \begin{pmatrix} -\xi + \xi^4 & \xi^2 - \xi^3 \\ \xi^2 - \xi^3 & \xi - \xi^4 \end{pmatrix} \\ &= \frac{1}{5} \begin{pmatrix} \xi^2 + \xi^3 - 2 + \xi^4 + \xi - 2 & 0 \\ 0 & \xi^4 + \xi - 2 + \xi^2 + \xi^3 - 2 \end{pmatrix} \\ &= \frac{1}{5} \begin{pmatrix} -5 & 0 \\ 0 & -5 \end{pmatrix} \\ &= \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \end{aligned}$$

besitzt F die Ordnung 4. Ferner ist

$$\begin{aligned} EF &= -\begin{pmatrix} \xi^3 & 0 \\ 0 & \xi^2 \end{pmatrix} \cdot \frac{1}{\sqrt{5}} \begin{pmatrix} -\xi + \xi^4 & \xi^2 - \xi^3 \\ \xi^2 - \xi^3 & \xi - \xi^4 \end{pmatrix} \\ &= -\frac{1}{\sqrt{5}} \begin{pmatrix} -\xi^4 + \xi^2 & 1 - \xi \\ \xi^4 - 1 & \xi^3 - \xi \end{pmatrix}. \end{aligned}$$

Dabei ist

$$\begin{pmatrix} -\xi^4 + \xi^2 & 1 - \xi \\ \xi^4 - 1 & \xi^3 - \xi \end{pmatrix} \cdot \begin{pmatrix} -\xi^4 + \xi^2 & 1 - \xi \\ \xi^4 - 1 & \xi^3 - \xi \end{pmatrix} = \begin{pmatrix} 2\xi^4 + \xi^3 - \xi - 2 & -2\xi^4 + 2\xi^2 - \xi + 1 \\ \xi^4 - 2\xi^3 + 2\xi - 1 & -\xi^4 + \xi^2 + 2\xi - 2 \end{pmatrix}$$

und (unter Verwendung von $\xi^2 + \xi^3 = -\frac{1+\sqrt{5}}{2}$)

$$\begin{aligned} \begin{pmatrix} -\xi^4 + \xi^2 & 1 - \xi \\ \xi^4 - 1 & \xi^3 - \xi \end{pmatrix}^3 &= \begin{pmatrix} 2\xi^4 + \xi^3 - \xi - 2 & -2\xi^4 + 2\xi^2 - \xi + 1 \\ \xi^4 - 2\xi^3 + 2\xi - 1 & -\xi^4 + \xi^2 + 2\xi - 2 \end{pmatrix} \cdot \begin{pmatrix} -\xi^4 + \xi^2 & 1 - \xi \\ \xi^4 - 1 & \xi^3 - \xi \end{pmatrix} \\ &= \begin{pmatrix} 5\xi^4 - 5\xi^3 - 5\xi^2 + 5\xi & 0 \\ 0 & 5\xi^4 - 5\xi^3 - 5\xi^2 + 5\xi \end{pmatrix} \end{aligned}$$

$$\begin{aligned} &= \begin{pmatrix} -5-10\left(\xi^3+\xi^2\right) & 0 \\ 0 & -5-10\left(\xi^3+\xi^2\right) \end{pmatrix} \\ &= \begin{pmatrix} 5\sqrt{5} & 0 \\ 0 & 5\sqrt{5} \end{pmatrix}, \end{aligned}$$

also ist

$$(EF)^3 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

und die Ordnung von EF ist 6. Diese Gruppe besitzt 120 Elemente und heißt die , sie wird mit BI bezeichnet.

Untergruppen der speziellen unitären Gruppe

In den oben aufgelisteten endlichen Untergruppen der $\mathrm{SL}_2(\mathbb{C})$ sind die (erzeugenden) Matrizen von der Form

$$\begin{pmatrix} u & -\overline{v} \\ v & \overline{u} \end{pmatrix},$$

d.h. es handelt sich um unitäre Matrizen. Wir erinnern an die entsprechenden Begrifflichkeiten. Das Standardskalarprodukt auf dem $\mathbb{C}^n$ ist durch

$$\langle w, z \rangle = \sum_{i=1}^{n} w_i \overline{z_i}$$

definiert. Eine lineare Abbildung $f\colon \mathbb{C}^n \to \mathbb{C}^n$ heißt *unitär*, wenn sie das Standardskalarprodukt respektiert, wenn also

$$\langle f(w), f(z) \rangle = \langle w, z \rangle$$

für alle $w, z \in \mathbb{C}^n$ gilt. Dies ist das komplexe Analogon zu den Isometrien im Reellen.

Definition 23.6. Der $\mathbb{C}^n$ sei mit dem komplexen Standardskalarprodukt versehen. Die Menge aller unitären linearen Abbildungen $f\colon \mathbb{C}^n \to \mathbb{C}^n$ bilden eine Gruppe, die die *unitäre Gruppe* heißt. Sie wird mit $\mathrm{U}_n(\mathbb{C})$ bezeichnet.

Definition 23.7. Der $\mathbb{C}^n$ sei mit dem komplexen Standardskalarprodukt versehen. Die Menge aller unitären linearen Abbildungen $f\colon \mathbb{C}^n \to \mathbb{C}^n$ mit Determinante 1 bilden eine Gruppe, die die *spezielle unitäre Gruppe* heißt. Sie wird mit $\mathrm{SU}_n(\mathbb{C})$ bezeichnet.

Lemma 23.8. *Jede endliche Untergruppe $G \subseteq \mathrm{SL}_n(\mathbb{C})$ ist zu einer Untergruppe der $\mathrm{SU}_n(\mathbb{C})$ konjugiert.*

Beweis. Es sei $\langle -, - \rangle$ das Standardskalarprodukt auf dem $\mathbb{C}^n$. Wir definieren zuerst unter Bezug auf die endliche Gruppe

$$G \subseteq \mathrm{SL}_n(\mathbb{C})$$

ein neues Skalarprodukt auf $\mathbb{C}^n$, nämlich

$$\Phi(w,z) := \frac{1}{\#(G)} \sum_{\sigma \in G} \langle \sigma w, \sigma z \rangle .$$

Nach Aufgabe 23.6 handelt es sich in der Tat um ein Skalarprodukt. Für ein Gruppenelement $\tau \in G$ ist ferner

$$\Phi(\tau w, \tau z) = \frac{1}{\#(G)} \sum_{\sigma \in G} \langle \sigma\tau w, \sigma\tau z \rangle = \frac{1}{\#(G)} \sum_{\sigma \in G} \langle \sigma w, \sigma z \rangle = \Phi(w,z),$$

da ja insgesamt über die gleichen Gruppenelemente aufsummiert wird. Die zu G gehörenden linearen Abbildungen sind also unitär bezüglich Φ. Es sei $u_1, \ldots, u_n$ eine Orthonormalbasis von $\mathbb{C}^n$ bezüglich Φ und sei M die Matrix, deren Spalten die u_i sind. Wir betrachten die konjugierte Gruppe

$$H := M^{-1}GM,$$

also

$$H = \left\{ M^{-1}\sigma M | \, \sigma \in G \right\}.$$

Dabei gilt die Beziehung

$$\langle w, z \rangle = \Phi(Mw, Mz),$$

da dies für die Standardbasis git. Für $\tau \in H$ und $w, z \in \mathbb{C}^n$ gilt

$$\begin{aligned} \langle \tau w, \tau z \rangle &= \left\langle M^{-1}\sigma M w, M^{-1}\sigma M z \right\rangle \\ &= \Phi(\sigma M w, \sigma M z) \\ &= \Phi(Mw, Mz) \\ &= \langle w, z \rangle , \end{aligned}$$

d.h. H ist bezüglich des Standardskalarproduktes unitär. Wegen

$$\tau = M^{-1}\sigma M$$

und $\sigma \in \mathrm{SL}_n(\mathbb{C})$ besitzt auch τ die Determinante 1, und daher ist $H \subseteq \mathrm{SU}_n(\mathbb{C})$. □

23. Arbeitsblatt

Aufwärmaufgaben

Aufgabe 23.1. Es sei $\zeta \in \mathbb{C}$ eine n-te primitive Einheitswurzel. Zeige, dass die zyklische Gruppe

$$Z_n = \left\{ \begin{pmatrix} \zeta^j & 0 \\ 0 & \zeta^{-j} \end{pmatrix} | \, j = 0, \ldots, n-1 \right\} \subseteq \mathrm{SL}_2(\mathbb{C})$$

auf der Punktmenge

$$\left\{ \begin{pmatrix} \zeta^j \\ \zeta^{-j} \end{pmatrix} | \, j = 0, \ldots, n-1 \right\}$$

treu operiert, dass sie bei n ungerade auf der Geradenmenge

$$\left\{ \langle \begin{pmatrix} \zeta^j & \\ & \zeta^{-j} \end{pmatrix} \rangle \mid j = 0, \ldots, n-1 \right\}$$

ebenfalls treu operiert und dass sie bei n gerade auf der Geradenmenge

$$\left\{ \langle \begin{pmatrix} \zeta^j & \\ & \zeta^{-j} \end{pmatrix} \rangle \mid j = 0, \ldots, \frac{n}{2} - 1 \right\}$$

operiert, aber nicht treu. Was ist in diesem Fall der Kern der Operation?

Aufgabe 23.2. Wir betrachten die binäre Diedergruppe BD_n. Zeige, dass bei $n \geq 3$ die von

$$B = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

erzeugte Untergruppe kein Normalteiler ist.

Aufgabe 23.3. Es sei $\zeta \in \mathbb{C}$ eine $2n$-te primitive Einheitswurzel. Zeige, dass die binäre Diedergruppe BD_n auf der Geradenmenge

$$\left\{ \langle \begin{pmatrix} \zeta^j & \\ & \zeta^{-j} \end{pmatrix} \rangle \mid j = 0, \ldots, n-1 \right\} \cup \{ \langle \begin{pmatrix} 1 \\ 0 \end{pmatrix} \rangle, \langle \begin{pmatrix} 0 \\ 1 \end{pmatrix} \rangle \}$$

operiert.

Aufgabe 23.4. Zeige, dass die in Beispiel 23.1, Beispiel 23.2, Beispiel 23.3 und Beispiel 23.4 beschriebenen Gruppen bereits Untergruppen der $\mathrm{SU}_2(\mathbb{C})$ sind.

Aufgabe 23.5. Zeige, dass die Matrix

$$F = \frac{1}{\sqrt{5}} \begin{pmatrix} -\xi + \xi^4 & \xi^2 - \xi^3 \\ \xi^2 - \xi^3 & \xi - \xi^4 \end{pmatrix}$$

zu $\mathrm{SU}_2(\mathbb{C})$ gehört.

Aufgabe 23.6. Es sei $G \subseteq \mathrm{GL}_n(\mathbb{C})$ eine endliche Untergruppe und es sei $\langle -, - \rangle$ das Standardskalarprodukt auf dem $\mathbb{C}^n$. Zeige, dass durch

$$\Phi(w, z) := \frac{1}{\#(G)} \sum_{\sigma \in G} \langle \sigma w, \sigma z \rangle$$

ein Skalarprodukt auf $\mathbb{C}^n$ definiert wird.

Aufgabe 23.7. Es sei $M \in \mathrm{Mat}_n(\mathbb{C})$ eine Matrix und

$$\varphi\colon\ \mathbb{C}^n \longrightarrow \mathbb{C}^n$$

die zugehörige lineare Abbildung. Zeige, dass φ genau dann unitär ist, wenn ${}^tM \cdot \overline{M}$ die Einheitsmatrix ist.

In den folgenden Aufgaben rekapitulieren wir einige Eigenschaften der Einheitswurzeln und der Kreisteilungspolynome.

Aufgabe 23.8. Bestimme die Koordinaten der fünften Einheitswurzeln in $\mathbb{C}$.

Aufgabe 23.9. Sei $n \in \mathbb{N}_+$. Zeige, dass die n Vektoren (im $\mathbb{C}^n$)

$$(1, \zeta, \zeta^2, \ldots, \zeta^{n-1}), \zeta \in \mu_n(\mathbb{C}),$$

linear unabhängig sind.

Aufgabe 23.10. Es sei $\zeta \in K$ eine n-te primitive Einheitswurzel in einem Körper K. Zeige die „Schwerpunktformel“

$$1 + \zeta + \zeta^2 + \ldots + \zeta^{n-1} = 0.$$

Aufgabe 23.11. Bestimme die Kreisteilungspolynome Φ_n für $n \leq 15$.

Aufgaben zum Abgeben

Aufgabe 23.12. (2 Punkte)

Bestimme die Eigenwerte und die Eigenvektoren der Matrix

$$\frac{1}{\sqrt{2}} \begin{pmatrix} \zeta^7 & \zeta 7 \\ \zeta^5 & \zeta \end{pmatrix}$$

mit $\zeta = \frac{1+i}{\sqrt{2}}$.

Aufgabe 23.13. (3 Punkte)

Zeige, dass die Matrix

$$\frac{1}{\sqrt{2}} \begin{pmatrix} i & -i \\ \zeta & -i \end{pmatrix}$$

zur binären Oktaedergruppe gehört (dabei ist ζ eine primitive achte Einheitswurzel). Gehört sie auch zur binären Tetraedergruppe?

Aufgabe 23.14. (6 Punkte)

Zeige, dass die binäre Ikosaedergruppe 120 Elemente besitzt.

24. Vorlesung - Ebene komplexe Gruppen II

Die Beziehung zwischen $\mathrm{SL}_2(\mathbb{C})$ und $\mathrm{SO}_3(\mathbb{R})$

Für die Klassifikation der endlichen Untergruppen der $\mathrm{SL}_2(\mathbb{C})$ werden wir die platonische Klassifikation der endlichen Untergruppen der $\mathrm{SO}_3(\mathbb{R})$ heranziehen. Die Beziehung zwischen diesen beiden Fragestellungen beruht darauf, dass einerseits die $\mathrm{SL}_2(\mathbb{C})$ auf der komplex-projektiven Geraden $\mathbb{P}^1_{\mathbb{C}}$ und andererseits die Isometrien des $\mathbb{R}^3$ auf der 2-Sphäre $S^2 \subseteq \mathbb{R}^3$ operiert. Die Homöomorphie $\mathbb{P}^1_{\mathbb{C}} \cong S^2$ ermöglicht einen Zusammenhang zwischen diesen Gruppen und ihren endlichen Untergruppen.

Die projektive komplexe Gerade $\mathbb{P}^1_{\mathbb{C}}$ ist die Menge aller Geraden im $\mathbb{C}^2$ durch den Nullpunkt; sie ist topologisch betrachtet eine Sphäre S^2. Diesen Zusammenhang kann man explizit machen, indem man als Zwischenschritt mit $\mathbb{C} \cup \{\infty\}$ arbeitet. Diese erweiterte komplexe Ebene steht einerseits mit der projektiven Geraden ($\mathbb{C}$ ist eine affine Karte der projektiven Gerade, die den „unendlich fernen Punkt“ ∞ nicht enthält) und andererseits mit der Sphäre über die stereographische Projektion in Bijektion (∞ entspricht dabei dem Nordpol).

Eine komplexe Zahl $u \in \mathbb{C}$ definiert die von $(u, 1) \in \mathbb{C}^2$ erzeugte Gerade und damit den Punkt (in homogenen Koordinaten) $(u : 1)$ der komplex-projektiven Geraden $\mathbb{P}^1_{\mathbb{C}}$. Die Umkehrabbildung ist durch $(u : v) \mapsto \frac{u}{v}$ gegeben, die für $v \neq 0$ definiert ist. Dem Punkt $(1, 0)$ entspricht der unendlich ferne Punkt ∞.

Die Umkehrabbildung der stereographischen Projektion ist die Abbildung

$$\begin{aligned}\mathbb{C} \cong \mathbb{R}^2 \longrightarrow S^2 \setminus \{N\} z = a + bi &\longmapsto \frac{1}{1 + |z|^2} \\ \left(2\,\mathrm{Re}\,(z)\,,\, 2\,\mathrm{Im}\,(z)\,,\, |z|^2 - 1\right) &= \frac{1}{1 + a^2 + b^2}\left(2a,\, 2b,\, a^2 + b^2 - 1\right).\end{aligned}$$

Die Gesamtabbildung

$$\mathbb{P}^1_{\mathbb{C}} \setminus \{(1:0)\} \longrightarrow \mathbb{C} \longrightarrow S^2 \setminus \{N\}$$

besitzt insgesamt die Beschreibung

$$(u : v) \longmapsto \frac{1}{1 + \left|\frac{u}{v}\right|^2}\left(2\,\mathrm{Re}\,\left(\frac{u}{v}\right),\, 2\,\mathrm{Im}\,\left(\frac{u}{v}\right),\, \left|\frac{u}{v}\right|^2 - 1\right).$$

Mit $u = a + bi$ und $v = c + di$ schreibt man dies (unter Verwendung von $|v|^2 = v\overline{v}$) als

$$\begin{aligned}&\frac{1}{1 + \left|\frac{u}{v}\right|^2}\left(2\,\mathrm{Re}\,\left(\frac{u}{v}\right),\, 2\,\mathrm{Im}\,\left(\frac{u}{v}\right),\, \left|\frac{u}{v}\right|^2 - 1\right) \\ = \;& \frac{1}{|u|^2 + |v|^2}\left(2\,\mathrm{Re}\,(u\overline{v})\,,\, 2\,\mathrm{Im}\,(u\overline{v})\,,\, |u|^2 - |v|^2\right)\end{aligned}$$

$$= \frac{1}{a^2+b^2+c^2+d^2}\left(2ac+2bd,\, 2bc-2ad,\, a^2+b^2-c^2-d^2\right).$$

Diese Formel zeigt, dass die Abbildung für alle $(u:v) \in \mathbb{P}^1_{\mathbb{C}}$ definiert ist, wobei $(1:0)$ auf den Nordpol $(0,0,1)$ abgebildet wird. Es liegt also eine explizite Bijektion $\mathbb{P}^1_{\mathbb{C}} \to S^2$ vor. Die Umkehrabbildung ist (für $(x_1,x_2,x_3) \neq (0,0,1)$ mit $x_1^2+x_2^2+x_3^2=1$) durch

$$(x_1,x_2,x_3) \longmapsto (x_1+x_2 i : 1-x_3)$$

gegeben. Wenn man eine normierte Repräsentierung dieses Punktes erhalten möchte, so muss man durch $\sqrt{2-2x_3}$ dividieren.

Insbesondere erhält man eine explizite (in den natürlichen Topologien stetige) Abbildung

$$\mathbb{C}^2 \setminus \{(0,0)\} \longrightarrow S^2,$$

deren Fasern genau die punktierten komplexen Geraden sind.

Die natürliche Operation der $\mathrm{GL}_2(\mathbb{C})$ auf $\mathbb{C}^2$ - und das gilt auch für jede endliche Untergruppe $G \subseteq \mathrm{GL}_2(\mathbb{C})$ - induziert eine Operation auf der Menge der eindimensionalen Untervektorräume (also der komplexen Geraden durch den Nullpunkt) und damit auf $\mathbb{P}^1_{\mathbb{C}}$. Eine Gerade $H \subseteq \mathbb{C}^2$ wird durch $\sigma \in \mathrm{GL}_2(\mathbb{C})$ einfach auf die Bildgerade $\sigma(H)$ abgebildet. Eine Gerade $\langle (u,v) \rangle$ wird unter $\sigma = \begin{pmatrix} \ell & m \\ n & p \end{pmatrix}$ auf die Gerade $\langle (\ell u + mv, nu+pv) \rangle$ abgebildet, bzw. in homogenen Koordinaten

$$(u:v) \longmapsto (\ell u + mv : nu + pv).$$

Dabei wirken Streckungen, also Abbildungen der Form $\begin{pmatrix} s & 0 \\ 0 & s \end{pmatrix}$ mit $s \neq 0$, trivial auf der Menge der Geraden und auf der projektiven Geraden. Da man jede invertierbare Matrix als Produkt einer solchen Streckungsmatrix und einer invertierbaren Matrix mit Determinante 1 schreiben kann, muss man im Wesentlichen die Operation der $\mathrm{SL}_2(\mathbb{C})$ auf der projektiven Geraden verstehen. Die einzige Matrix $M \in \mathrm{SL}_2(\mathbb{C})$ neben der Einheitsmatrix, die sämtliche Geraden auf sich selbst abbildet, ist

$$-E_2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Definition 24.1. Es sei K ein Körper und $n \in \mathbb{N}$. Die Restklassengruppe

$$\mathrm{SL}_n(K) \,/\, \left(K^\times \cdot \mathrm{Id} \cap \mathrm{SL}_n(K)\right)$$

heißt *projektive spezielle lineare Gruppe*. Sie wird mit

$$\mathrm{PSL}_n(K)$$

bezeichnet.

Insbesondere ist $\mathrm{PSL}_2(\mathbb{C}) \cong \mathrm{SL}_2(\mathbb{C})/\{\pm E_2\}$. Diese Gruppe operiert in natürlicher Weise treu und transitiv auf der projektiven Geraden. Mittels der obigen Identifizierung $\mathbb{P}^1_{\mathbb{C}} \cong S^2$ kann man die Operation der Gruppen (und Untergruppen) $\mathrm{GL}_2(\mathbb{C})$, $\mathrm{SL}_2(\mathbb{C})$, $\mathrm{PSL}_2(\mathbb{C})$ auf $\mathbb{P}^1_{\mathbb{C}}$ zu einer Operation dieser Gruppen auf der zweidimensionalen Sphäre übersetzen. Es stellt sich heraus, dass die zugehörigen Automorphismen im Allgemeinen nicht längentreu sind. Um dies zu erreichen, arbeiten wir mit der unitären Gruppen $\mathrm{SU}_2(\mathbb{C})$.

Satz 24.2. *Es gibt einen surjektiven Gruppenhomomorphismus*

$$\mathrm{SU}_2(\mathbb{C}) \longrightarrow \mathrm{SO}_3(\mathbb{R}),$$

dessen Kern gleich

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

ist. Die Abbildung kann explizit (mit $u = a + bi$ und $v = c + di$ unter der Bedingung $a^2 + b^2 + c^2 + d^2 = 1$) durch

$$\begin{pmatrix} u & -\overline{v} \\ v & \overline{u} \end{pmatrix} \longmapsto \begin{pmatrix} a^2+b^2-c^2-d^2 & 2(-ad+bc) & 2(ac+bd) \\ 2(ad+bc) & a^2-b^2+c^2-d^2 & 2(-ab+cd) \\ 2(-ac+bd) & 2(ab+cd) & a^2-b^2-c^2+d^2 \end{pmatrix}$$

realisiert werden.

Beweis. Es sei

$$\varphi\colon\ \mathbb{P}^1_{\mathbb{C}} \longrightarrow S^2$$

die explizite Homöomorphie zwischen der komplex-projektiven Geraden und der 2-Sphäre S^2. Durch

$$\mathrm{GL}_2(\mathbb{C}) \longrightarrow \mathrm{Aut}\left(S^2\right), \sigma \longmapsto \varphi^{-1}\sigma \circ \varphi,$$

erhält man einen Gruppenhomomorphismus der allgemeinen linearen Gruppe in die Gruppe der stetigen Automorphismen (also der Homöomorphismen) der Sphäre. Eine explizite Rechnung für $\sigma \in \mathrm{SU}_2(\mathbb{C})$ zeigt, dass der zugehörige Homöomorphismus von einer linearen Abbildung der angegebenen Gestalt herrührt. Zur Surjektivität Für $v = 0$ und $u = a + bi$ mit $a^2 + b^2 = 1$ geht die Matrix links auf

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & a^2-b^2 & -2ab \\ 0 & 2ab & a^2-b^2 \end{pmatrix}.$$

Wenn man $s = \cos\alpha$ und $t = \sin\alpha$ vorgibt und $a = \frac{\sqrt{s+1}}{\sqrt{2}}$ und $b = \pm\frac{\sqrt{1-s}}{\sqrt{2}}$ setzt (das Vorzeichen ist geeignet zu wählen), so wird die Matrix zu

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\alpha & -\sin\alpha \\ 0 & \sin\alpha & \cos\alpha \end{pmatrix},$$

d.h. sie beschreibt die Drehung um den Winkel α um die x-Achse. Diese Drehung liegt also im Bild der Abbildung. Indem man die Rollen von a, b, c,

d ändert, sieht man, dass auch die Drehungen um die beiden anderen Koordinatenachsen im Bild der Abbildung liegen. Nach Aufgabe 24.11 lässt sich jede Isometrie als eine Verknüpfung von Drehungen um die Koordinatenachsen erhalten. Also ist die Abbildung surjektiv. Zur Bestimmung des Kerns addieren wir jeweils die beiden Einträge der Matrix, die nicht auf der Diagonalen liegen und symmetrisch zur Diagonalen sind. Dies ergibt die Bedingungen $bc = bd = cd = 0$. Die Differenzen von je zwei Einträgen der Diagonalen ergibt die Bedingung $b^2 = c^2 = d^2 = 0$, woraus insgesamt $b = c = d = 0$ folgt. Die Bedingung $a^2 = 1$ führt dann zu den beiden Elementen im Kern. □

Lemma 24.3. *Das einzige Element aus* $\mathrm{SU}_2(C)$ *der Ordnung* 2 *ist* $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$.

Beweis. Sei

$$M = \begin{pmatrix} u & -\overline{v} \\ v & \overline{u} \end{pmatrix}$$

mit $u = a + bi$, $v = c + di$ und mit $M^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Das bedeutet

$$\begin{pmatrix} u & -\overline{v} \\ v & \overline{u} \end{pmatrix} \begin{pmatrix} u & -\overline{v} \\ v & \overline{u} \end{pmatrix} = \begin{pmatrix} u^2 - v\overline{v} & -u\overline{v} - \overline{uv} \\ uv + \overline{u}v & -v\overline{v} + \overline{uu} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Wir nehmen zunächst $v \neq 0$ an. Daraus folgt $u + \overline{u} = 0$, also ist der Realteil von u gleich 0. Daher ist u imaginär und sein Quadrat ist negativ. Dann ist aber auch $u^2 - v\overline{v}$ negativ und nicht gleich 1. Also ist $v = 0$. Dann ist $u^2 = 1$ und somit ist $u = \pm 1$. □

Satz 24.4. *Die endlichen Untergruppen der* $\mathrm{SL}_2(\mathbb{C})$ *sind bis auf Isomorphie (und bis auf Konjugation)*

(1) *die endlichen zyklischen Gruppen* Z_n,
(2) *die binären Diedergruppen* BD_n, $n \geq 2$,
(3) *die binäre Tetraedergruppe* BT,
(4) *die binäre Oktaedergruppe* BO,
(5) *die binäre Ikosaedergruppe* BI.

Beweis. Nach Lemma 23.8 können wir davon ausgehen, dass $G \subseteq \mathrm{SU}_2(\mathbb{C})$ ist. Es sei

$$\pi\colon\ \mathrm{SU}_2(\mathbb{C}) \longrightarrow \mathrm{SO}_3(\mathbb{R})$$

der surjektive Gruppenhomomorphismus aus Satz 24.2. Es sei $H = \pi(G)$ die Bildgruppe von G unter dieser Abbildung, für die es aufgrund von Satz 22.8 starke Einschränkungen gibt. Wenn $\#(G)$ ungerade ist, so enthält G kein Element der Ordnung 2. Also ist $G \cap (\text{kern } \pi)$ trivial und somit ist $G \to H$ ein

Isomorphismus. Aufgrund der Klassifikation für endliche Symmetriegruppen muss G zyklisch sein. Sei also $\#(G)$ gerade, sagen wir $\#(G) = 2^m u$ mit u ungerade. Nach dem Satz von Sylow besitzt G eine Untergruppe mit 2^m Elmenten und damit insbesondere auch ein Element der Ordnung 2. Wegen Satz 24.3 gibt es in $\mathrm{SU}_2(\mathbb{C})$ nur das Element $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ der Ordnung 2. Also ist $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \in G$ und somit ist kern $\pi \subseteq G$. Damit ist insbesondere

$$G = \pi^{-1}(\pi(G)),$$

d.h. G ist das Urbild zu einer endlichen Untergruppe $H \subseteq \mathrm{SO}_3(\mathbb{R})$. H ist also eine der Untergruppen aus der Liste von Satz 22.8. Zwei isomorphe Gruppen $H_1, H_2 \subseteq \mathrm{SO}_3(\mathbb{R})$ sind sogar konjugiert. Wenn $\alpha \in \mathrm{SO}_3(\mathbb{R})$ den inneren Automorphismus stiftet und $\tilde{\alpha} \in \mathrm{SU}_2(\mathbb{C})$ ein Urbild ist, so vermittelt $\tilde{\alpha}$ einen Isomorphismus der Urbildgruppen $\pi^{-1}(H_1)$ und $\pi^{-1}(H_2)$. Der Isomorphietyp von G ist also durch $\pi(G)$ festgelegt. Wenn $\pi(G) = D_n, T, O, I$ ist, so muss $G = BD_n, BT, BO, BI$ sein, da der Isomorphietyp festgelegt ist und die in den definierenden Beispielen Beispiel 23.2, Beispiel 23.4, Beispiel 23.3 und Beispiel 23.5 modulo dem Element der Ordnung 2 die entsprechenden reellen Symmetriegruppen ergeben. □

Quotientensingularitäten

Definition 24.5. Es sei K ein Körper und $G \subseteq \mathrm{GL}_n(K)$ eine endliche Untergruppe. Dann nennt man den Invariantenring $K[X_1, \ldots, X_n]^G$ (bzw. sein Spektrum) eine *Quotientensingularität*.

Definition 24.6. Es sei K ein Körper und $G \subseteq \mathrm{SL}_n(K)$ eine endliche Untergruppe. Dann nennt man den Invariantenring $K[X_1, \ldots, X_n]^G$ (bzw. sein Spektrum) eine *spezielle Quotientensingularität*.

Diese beiden Definitionen umfassen als Extremfall auch die Situation, wo der Invariantenring regulär ist, also im strengen Sinn überhaupt keine Singularität vorliegt. Es kann sein, dass ein kommutativer Ring sowohl zum Invariantenring zu $G \subseteq \mathrm{GL}_n(K)$, $G \not\subseteq \mathrm{SL}_n(K)$, als auch zum Invariantenring zu $H \subseteq \mathrm{SL}_n(K)$ isomorph ist. Ein Beispiel dafür ist der Polynomring selbst. Ein Beispiel für eine Quotientensingularität, die keine spezielle Quotientensingularität ist, ist der Veronesering $K[U, V]^{(k)}$, $k \geq 3$, den wir in Beispiel 9.12 vorgestellt haben. Wir haben bisher noch nicht gezeigt, dass diese für $k \geq 3$ nicht auch als ein Invariantenring zu einer Operation einer Untergruppe der speziellen linearen Gruppe realisiert werden kann. Dies wird sich als Nebenresultat der Berechnungen der nächsten Vorlesungen ergeben.

24. Arbeitsblatt

Aufwärmaufgaben

Aufgabe 24.1. Sei $n \in \mathbb{N}_+$ und $\alpha = \frac{360}{n}$. Betrachte die Untergruppe der Drehmatrizen

$$G = \left\{ \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}^j \mid j = 0, \ldots, n-1 \right\} \subseteq \mathrm{SL}_2(\mathbb{R}) .$$

Zeige, dass diese Gruppe, aufgefasst in $\mathrm{SL}_2(\mathbb{C})$, konjugiert zu Z_n aus Beispiel 23.1 ist.

Aufgabe 24.2. Es sei $G \subseteq \mathrm{GL}_n(K)$ eine Untergruppe der allgemeinen linearen Gruppe über einem Körper K und $K \subseteq L$ eine Körpererweiterung. Zeige

$$K[X_1, \ldots, X_n]^G = K[X_1, \ldots, X_n] \cap L[X_1, \ldots, X_n]^G.$$

Aufgabe 24.3. Betrachte die Untergruppe der Drehmatrizen, die durch die Vierteldrehung

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

erzeugt wird. Bestimme den reellen und den komplexen Invariantenring zur zugehörigen linearen Operation.

Aufgabe 24.4. Bestimme zu einer speziellen unitären Matrix

$$\begin{pmatrix} u & -\overline{v} \\ v & \overline{u} \end{pmatrix} \in \mathrm{SU}_2(\mathbb{C})$$

die Eigenwerte und die Eigenvektoren.

Aufgabe 24.5. Zeige, dass zu einer speziellen unitären Matrix

$$\begin{pmatrix} u & -\overline{v} \\ v & \overline{u} \end{pmatrix} \in \mathrm{SU}_2(\mathbb{C})$$

die beiden Eigenvektoren, aufgefasst in $\mathbb{P}^1_{\mathbb{C}} \cong S^2$, antipodal sind.

Aufgabe 24.6. Zeige, dass zu einer diagonalisierbaren Matrix

$$\begin{pmatrix} u & v \\ w & z \end{pmatrix} \in \mathrm{SL}_2(\mathbb{C})$$

die beiden Eigenvektoren, aufgefasst in $\mathbb{P}^1_{\mathbb{C}} \cong S^2$, nicht antipodal sein müssen.

Aufgabe 24.7. Überprüfe, dass die in Vorlesung 24 angegebenen Abbildungen eine Homöomorphie zwischen $\mathbb{P}^1_{\mathbb{C}}$ und S^2 stiften.

Aufgabe 24.8. Es sei G eine Gruppe, die auf einer Menge M operiere, und es sei $\psi\colon\ M \to N$ eine Bijektion. Zeige, dass dann auch eine natürliche Operation von G auf N vorliegt.

Aufgabe 24.9. Es sei $M \in \mathrm{SL}_2(\mathbb{C})$ eine spezielle lineare Matrix mit der zugehörigen Abbildung

$$\varphi\colon\ \mathbb{P}^1_{\mathbb{C}} \cong S^2 \longrightarrow \mathbb{P}^1_{\mathbb{C}} \cong S^2.$$

Zeige, dass φ keine längentreue Abbildung und nicht zu einer linearen Abbildung von $\mathbb{R}^3$ nach $\mathbb{R}^3$ fortsetzbar sein muss.

Aufgabe 24.10. Seien a, b, c, d reelle Zahlen mit

$$a^2 + b^2 + c^2 + d^2 \ = \ 1.$$

Zeige, das die Determinante der Matrix

$$\begin{pmatrix} a^2+b^2-c^2-d^2 & 2(-ad+bc) & 2(ac+bd) \\ 2(ad+bc) & a^2-b^2+c^2-d^2 & 2(-ab+cd) \\ 2(-ac+bd) & 2(ab+cd) & a^2-b^2-c^2+d^2 \end{pmatrix}$$

gleich 1 ist.

Aufgabe 24.11. Zeige, dass sich jede lineare Isometrie des $\mathbb{R}^3$ als Verknüpfung von Drehungen um die drei Koordinantenachsen realisieren lässt.

Aufgabe 24.12. Zeige, dass man die Kleinsche Vierergruppe nicht als Untergruppe der $\mathrm{SL}_2(\mathbb{C})$, wohl aber als Untergruppe der $\mathrm{GL}_2(\mathbb{C})$ realisieren kann.

Aufgabe 24.13. Man gebe ein Beispiel von zwei endlichen Untergruppen $G, H \subseteq \mathrm{GL}_2(\mathbb{C})$, die zueinander isomorph, aber nicht zueinander konjugiert sind.

Aufgabe 24.14. Man gebe ein Beispiel von zwei endlichen Untergruppen $G, H \subseteq \mathrm{SL}_3(\mathbb{C})$, die zueinander isomorph, aber nicht zueinander konjugiert sind.

Aufgabe 24.15. Zeige, dass die binäre Ikosaedergruppe nicht isomorph zur Permutationsgruppe S_5 ist.

Aufgabe 24.16. Bestimme die Ordnungen der Elemente der binären Ikosaedergruppe.

Aufgaben zum Abgeben

Aufgabe 24.17. (10 Punkte)

Zeige, dass die in Beispiel 23.2, Beispiel 23.3, Beispiel 23.4 und Beispiel 23.5 beschriebenen Gruppen unter dem surjektiven Gruppenhomomorphismus

$$\mathrm{SU}_2(\mathbb{C}) \longrightarrow \mathrm{SO}_3(\mathbb{R})$$

die Urbildgruppen der entsprechenden reellen Gruppen sind.

25. Vorlesung - ADE Invarianten

Zur Berechnung der Invariantenringe

Wir möchten nun die Invariantenringe zu den zuvor klassifizierten Untergruppen der speziellen linearen Gruppe in der Dimension zwei berechnen. Eine typische Besonderheit der speziellen Quotientensingularitäten in der Dimension zwei ist, dass sie sich mit einer einzigen Gleichung beschreiben lassen. Diese Gleichungen wollen wir im Folgenden bestimmen.

Satz 25.1. *Es sei $G \subseteq \mathrm{SU}_2(\mathbb{C})$ eine endliche Untergruppe mit ihrer natürlichen Operation auf dem Polynomring $\mathbb{C}[U,V]$. Es sei $H = \pi(G)$ die zugehörige Untergruppe von $\mathrm{SO}_3(\mathbb{R})$ und es sei K eine Bahn zur Operation von H auf der Sphäre S^2, die wir auch mit der komplex-projektiven Geraden $\mathbb{P}^1_{\mathbb{C}}$ und der Menge der eindimensionalen Untervektorräume in $\mathbb{C}^2$ identifizieren. Dann gelten folgende Aussagen.*

(1) *Zur Klasse K mit den darin enthaltenen Punkten (in $\mathbb{P}^1_{\mathbb{C}}$)*

$$(a_1 : b_1),\, (a_2 : b_2), \ldots, (a_r : b_r)$$

ist das Polynom

$$F := \prod_{j=1}^{r} (b_j U - a_j V)$$

G-semiinvariant.

(2) *Insbesondere ist zu einer Halbachsenklasse*

$$K = (a_1 : b_1),\ (a_2 : b_2), \ldots, (a_r : b_r)$$

das Polynom

$$F := \prod_{j=1}^{r} (b_j U - a_j V)$$

G-semiinvariant.

(3) *Wenn $F \in \mathbb{C}[U, V]$ ein homogenes, G-semiinvariantes Polynom mit der Faktorzerlegung*

$$F = \prod_{j=1}^{s} (d_j U - c_j V)$$

ist, und wenn $(c : d)$ einer dieser (Nullstellen)-Punkte ist, so ist auch $h(c : d)$ für $h \in H$ ein solcher Punkt.

Beweis. (1). Für $\sigma \in G$ ist

$$\begin{aligned} F\sigma &= \left(\prod_{j=1}^{r} (b_j U - a_j V) \right) \sigma \\ &= \prod_{j=1}^{r} \left((b_j U - a_j V)\, \sigma \right). \end{aligned}$$

Wir wissen, dass $\sigma \begin{pmatrix} a_j \\ b_j \end{pmatrix}$ projektiv betrachtet gleich einem der Punkte, sagen wir gleich $\begin{pmatrix} a_k \\ b_k \end{pmatrix}$, ist. Dies bedeutet, dass $\sigma \begin{pmatrix} a_j \\ b_j \end{pmatrix}$ und $\begin{pmatrix} a_k \\ b_k \end{pmatrix}$ den gleichen eindimensionalen Untervektorraum von $\mathbb{C}^2$ definieren, und daher ist

$$\sigma \begin{pmatrix} a_j \\ b_j \end{pmatrix} = \xi_j \begin{pmatrix} a_k \\ b_k \end{pmatrix}$$

mit einem gewissen $\xi_j \in \mathbb{C}^\times$. Da dies für jedes j gilt, und da die Wirkung von σ auf der zugrunde liegenden Punktmenge K bijektiv ist, also in $F\sigma$ die (bis auf Streckung) gleichen Linearfaktoren wie in F vorkommen, gilt

$$F\sigma = \zeta F$$

mit einem $\zeta = \prod_{j=1}^{r} \xi_j \in \mathbb{C}^\times$. Wir betrachten die Zuordnung

$$G \longrightarrow \mathbb{C}^\times,\ \sigma \longmapsto \frac{F\sigma}{F}.$$

Dies ist ein Charakter, wie man sieht, wenn man das Verhalten der einzelnen Faktoren betrachtet. Daher ist F eine Semiinvariante. (2) ist ein Spezialfall von (1). (3). Da F semiinvariant ist, ist insbesondere sein Nullstellengebilde, also die Vereinigung der Geraden zu den beteiligten Linearformen, invariant. Das Bild einer solchen Geraden unter $\sigma \in G$ muss also eine der Geraden sein.

Die Gleichheit von Geraden bedeutet aber, dass ihre zugehörigen Punkte auf der projektiven Gerade übereinstimmen. □

Die (Semi)-Invarianten zu den Halbachsenklassen sind besonders wichtig, da sie einen vergleichsweise kleinen Grad besitzen und häufig ein Algebraerzeugendensystem des Invariantenringes bilden.

Bemerkung 25.2. Satz 25.3 liefert die Grundlage zur Bestimmung der Invariantenringe unter den natürlichen Operationen der endlichen Untergruppen der $\mathrm{SU}_2(\mathbb{C})$. Insbesondere erlaubt dieser Satz folgende Strategie: Wenn G gar keine nichttrivialen Charaktere besitzt, so sind die im Satz konstruierten Semiinvarianten sogar Invarianten. Andernfalls gibt es einen nichttrivialen Charakter und damit einen surjektiven Gruppenhomomorphismus

$$\varphi\colon\ G \longrightarrow \mathbb{Z}/(r)$$

mit $r \geq 2$. Der Kern $N = \operatorname{kern} \varphi$ ist eine echte Untergruppe von G und kommt ebenfalls in der Liste aus Satz 24.4 vor, besitzt aber eine kleinere Ordnung. Da N ein Normalteiler in G ist, können wir den Invariantenring zu G aus dem Invariantenring zu N mittels Proposition 5.1 (3) ausrechnen.

Die Invariantenringe der zyklischen und der binären Diedergruppe

Der Invariantenring zur Operation der zyklischen Gruppe

$$G = \left\{ \begin{pmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{pmatrix} | \, \zeta^n = 1 \right\},$$

wobei ζ eine primitive n-te Einheitswurzel bezeichnet, wurde bereits in Beispiel 7.13 bestimmt. Es ist

$$K[U^n, V^n, UV] \ \cong\ K[X, Y, Z]/(XY - Z^n).$$

Diese Ringe nennt man A_{n+1}-*Singularitäten* (man beachte die Indizierung)! Darauf aufbauend können wir den Invariantenring zu den binären Diedergruppen BD_m bestimmen.

Beispiel 25.3. Es sei $m \in \mathbb{N}_+$ und es sei K ein Körper der Charakteristik $\neq 2$, der eine vierte primitive Einheitswurzel i und eine $2m$-te primitive Einheitswurzel ζ enthalte. Wir betrachten die von den Matrizen

$$A = \begin{pmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{pmatrix} \text{ und } B = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

erzeugte Untergruppe G (die man auch als BD_m bezeichnet) der $\mathrm{GL}_2(K)$ mit ihrer natürlichen Operation auf $R = K[U, V]$. Es sei $H \subseteq G$ die von A erzeugte zyklische Untergruppe der Ordnung $2m$. Da G die Ordnung $4m$

besitzt, ist H ein Normalteiler in G. Daher können wir mit Hilfe von Proposition 5.1 (3) und Beispiel 7.13 den Invariantenring $K[U,V]^G$ ausrechnen. Es ist ja

$$S := K[U,V]^H = K[U^{2m}, V^{2m}, UV] = K[X,Y,Z]/(XY - Z^{2m}).$$

Die Operation des nichttrivialen Elementes aus $G/H \cong \mathbb{Z}/(2)$ auf diesem Invariantenring wird durch die Operation von B auf $K[U,V]$ repräsentiert. Sie ist also durch $U \mapsto iV$ und $V \mapsto iU$ gegeben und induziert

$$X = U^{2m} \longmapsto i^{2m}V^{2m} = \rho Y\,,$$

$$Y = V^{2m} \longmapsto i^{2m}U^{2m} = \rho X\,,$$

$$Z = UV \longmapsto i^2 UV = -Z\,,$$

wobei $\rho = \pm 1$ ist, je nachdem, ob m gerade oder ungerade ist.

Durch diese Operation ist S $\mathbb{Z}/(2)$-graduiert. Bei m gerade sind

$$X + Y, Z^2, Z(X - Y)$$

invariante Polynome (bei m ungerade $X - Y, Z^2, Z(X + Y)$) und Z und $X - Y$ sind semiinvariante Polynome. Mittels $X = \frac{1}{2}(X+Y) + \frac{1}{2}(X-Y)$ und $Y = \frac{1}{2}(X+Y) - \frac{1}{2}(X-Y)$ lässt sich für jedes Monom $X^iY^jZ^k$ die homogene Zerlegung bezüglich dieser Graduierung angeben (wegen $(X-Y)^2 = (X+Y)^2 - 4Z^{2m}$ kann diese Invariante durch die anderen ausgedrückt werden). Deshalb bilden $L = X + Y$, $M = Z^2$, $N = Z(X - Y)$ ein Algebraerzeugendensystem des Invariantenringes

$$R^G = S^{\mathbb{Z}/(2)}.$$

Es besteht die Relation

$$\begin{aligned} N^2 &= Z^2(X-Y)^2 \\ &= M\left(X^2 + Y^2 - 2XY\right) \\ &= M\left(L^2 - 4XY\right) \\ &= ML^2 - 4MM^m \\ &= ML^2 - 4M^{m+1}. \end{aligned}$$

Da das Polynom

$$N^2 - ML^2 + 4M^{m+1}$$

irreduzibel ist, und der Invariantenring zweidimensional sein muss, ist

$$R^G \cong K[L,M,N]/(N^2 - ML^2 + 4M^{m+1}).$$

Unter schwachen Bedingungen an den Körper K ist dieser Ring isomorph zu

$$K[X,Y,Z]/(X^2 + YZ^2 + Y^{m+1})\,.$$

Man spricht von den D_{m+2}-*Singularitäten* (man beachte die Indizierung). Nach Aufgabe 25.9 ist D_3 isomorph zu A_3, also

$$\mathbb{C}[X,Y,Z]/(X^2+YZ^2+Y^2) \cong \mathbb{C}[S,T,U]/(ST+U^4),$$

so dass man diese D-Liste bei D_4 beginnen lässt. In den ursprünglichen Variablen U und V sind

$$U^{2m}+V^{2m},\ U^2V^2 \text{ und } UV(U^{2m}-V^{2m})$$

ein Algebraerzeugendensystem aus invarianten Polynomen.

Die Invarianten der binären Tetraedergruppe

Beispiel 25.4. Die binäre Diedergruppe BD_2 ist ein Normalteiler in der binären Tetraedergruppe BT. Die Untergruppenbeziehung kann man direkt aus den expliziten Beschreibungen

$$BD_2 = \langle \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \rangle \subseteq \langle \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} \zeta^7 & \zeta^7 \\ \zeta^5 & \zeta \end{pmatrix} \rangle = BT$$

(wobei ζ eine primitive achte Einheitswurzel ist) ablesen.

Beispiel 25.5. Wir wollen den Invariantenring zur binären Tetraedergruppe $\mathrm{BT} \subseteq \mathrm{SL}_2(\mathbb{C})$ berechnen, die auf dem Polynomring $\mathbb{C}[U,V]$ operiert. Wir verwenden den Normalteiler $\mathrm{BD}_2 \subseteq \mathrm{BT}$. Der Invariantenring $\mathbb{C}[U,V]^{\mathrm{BD}_2}$ wird nach Beispiel 25.5 von

$$L = U^4+V^4,\ M = U^2V^2 \text{ und } N = UV(U^4-V^4)$$

erzeugt mit der Relation

$$N^2 - ML^2 + 4M^3 = 0\,.$$

Auf diesem Invariantenring wirkt die Restklassengruppe $\mathrm{BT}/\mathrm{BD}_2 \cong \mathbb{Z}/(3)$, wobei das nichttriviale Element (die 1) durch

$$\frac{1}{\sqrt{2}} \begin{pmatrix} \zeta^7 & \zeta^7 \\ \zeta^5 & \zeta \end{pmatrix}$$

repräsentiert wird. Diese Matrix schickt U auf $\frac{1}{\sqrt{2}}(\zeta^7 U + \zeta^7 V)$ und V auf $\frac{1}{\sqrt{2}}(\zeta^5 U + \zeta V)$. Daher ist

$$U^4 \longmapsto -\frac{1}{4}\left(U^4+4U^3V+6U^2V^2+4UV^3+V^4\right)$$

und

$$V^4 \longmapsto -\frac{1}{4}(-U+V)^4 = -\frac{1}{4}\left(U^4-4U^3V+6U^2V^2-4UV^3+V^4\right)$$

und damit

$$L = U^4+V^4 \longmapsto -\frac{1}{2}\left(U^4+6U^2V^2+V^4\right) = -\frac{1}{2}L - 3M\,.$$

Ferner wird $M = U^2V^2$ auf

$$\begin{aligned}\frac{1}{4}\left(\zeta^7U+\zeta^7V\right)^2\left(\zeta^5U+\zeta V\right)^2 &= \frac{1}{4}\left(U+V\right)^2\left(-U+V\right)^2\\ &= \frac{1}{4}\left(U^4-2U^2V^2+V^4\right)\\ &= \frac{1}{4}\left(L-2M\right)\\ &= \frac{1}{4}L-\frac{1}{2}M\end{aligned}$$

geschickt. Das Element $N = UV\left(U^4-V^4\right)$ wird auf

$$\begin{aligned}\frac{1}{\sqrt{2}}\left(\zeta^7U+\zeta^7V\right)\frac{1}{\sqrt{2}}\left(\zeta^5U+\zeta V\right)\left(-2U^3V-2UV^3\right) &= (U+V)(-U+V)\left(-U^3V-UV^3\right)\\ &= (U+V)(-U+V)(-1)UV\left(U^2+V^2\right)\\ &= UV(U-V)(U+V)(U+iV)(U-iV)\\ &= UV\left(U^4-V^4\right)\\ &= N,\end{aligned}$$

also auf sich selbst geschickt. Neben

$$N = UV(U^4-V^4)$$

sind, wie man direkt nachrechnet, auch

$$P := L^2+12M^2 = U^8+14U^4V^4+V^8$$

und

$$Q := L^3-36LM^2 = U^{12}-33U^8V^4-33U^4V^8+V^{12}$$

invariant. Wegen

$$N^4 = \left(ML^2-4M^3\right)^2 = M^2L^4-8M^4L^2+16M^6$$

einerseits und

$$\begin{aligned}\left(L^3-36LM^2\right)^2-\left(L^2+12M^2\right)^3 &= -72L^4M^2+1296L^2M^4-36L^4M^2-432L^2M^4-1728M^6\\ &= -108L^4M^2+864L^2M^4-1728M^6\\ &= -108\left(M^2L^4-8M^4L^2+16M^6\right)\end{aligned}$$

andererseits haben wir zwischen diesen Invarianten die Relation

$$-108N^4 = \left(L^3-36LM^2\right)^2-\left(L^2+12M^2\right)^3.$$

Mit $P = L^2+12M^2$ und $Q = L^3-36LM^2$ liegt also die Relation

$$Q^2-P^3+108N^4 = 0$$

vor.

Wir müssen noch zeigen, dass damit alle Invarianten erfasst sind, dass also der Invariantenring von N, P, Q erzeugt wird. Dazu lassen wir uns davon leiten, dass eine Operation der $\mathbb{Z}/(3)$ vorliegt, die von einer $\mathbb{Z}/(3)$-Graduierung herrühren muss. Nach Korollar 7.11 ist der Invariantenring gleich dem Ring der neutralen Stufe, der häufig einfacher zu bestimmen ist.

Wie oben berechnet, wirkt der Erzeuger der Gruppe durch $L \mapsto -\frac{1}{2}L - 3M$ und $N \mapsto \frac{1}{4}L - \frac{1}{2}M$. Durch Diagonalisierung dieser Matrix erhält man, dass

$$A \;=\; \sqrt{3}iL - 6M$$

und

$$B \;=\; \sqrt{3}iL + 6M$$

Eigenvektoren zu den Eigenwerten $\frac{-1+\sqrt{3}i}{2}$ bzw. $\frac{-1-\sqrt{3}i}{2}$ sind, die dritte Einheitswurzeln sind. Wegen

$$L \;=\; \frac{1}{2\sqrt{3}i}(A+B)$$

und

$$M \;=\; \frac{1}{12}(B-A)$$

kann man die definierende Gleichung (des Invariantenringes zu BD_2) in den Variablen N, A, B als

$$\begin{aligned} N^2 - ML^2 + 4M^3 &= N^2 - \frac{1}{12}\left(\frac{1}{2\sqrt{3}i}\right)^2 (B-A)(A+B)^2 + 4\left(\frac{1}{12}\right)^3 (B-A)^3 \\ &= N^2 + \frac{1}{144}\left(B^3 + B^2A - BA^2 - A^3\right) + \frac{1}{432}\left(B^3 - 3B^2A + 3BA^2 - A^3\right) \\ &= N^2 + \frac{1}{108}\left(B^3 - A^3\right). \end{aligned}$$

Wir können also davon ausgehen, dass der Ring

$$K[N,A,B]/\left(N^2 + \frac{1}{108}B^3 - \frac{1}{108}A^3\right)$$

vorliegt, der $\mathbb{Z}/(3)$-graduiert ist, wobei N den Grad 0, B den Grad 1 und A den Grad 2 bekommt. Die definierende Gleichung besitzt den Grad 0. Der Ring der nullten Stufe wird offenbar von N, A^3, B^3, AB erzeugt. Für die oben gefundenen invarianten Polynome gilt

$$\begin{aligned} P &= L^2 + 12M^2 \\ &= -\frac{1}{12}(A+B)^2 + \frac{1}{12}(B-A)^2 \\ &= -\frac{1}{3}AB \end{aligned}$$

und

$$\begin{aligned} Q &= L^3 - 36LM^2 \\ &= \frac{1}{2\sqrt{3}i}(A+B)\left(-\frac{1}{12}(A+B)^2 - \frac{1}{4}(B-A)^2\right) \\ &= \frac{1}{6\sqrt{3}i}(A+B)\left(-A^2 + AB - B^2\right) \\ &= \frac{1}{6\sqrt{3}i}\left(A^3 + B^3\right). \end{aligned}$$

Mit Hilfe der Relation kann man A^3 (und B^3) als Linearkombination von N, P, Q ausdrücken. Daher sind dies Algebraerzeuger des Invariantenrings und dieser ist zu

$$\mathbb{C}[X,Y,Z]/(X^2+Y^3+Z^4)$$

isomorph. Man spricht von der E_6-*Singularität*.

25. Arbeitsblatt

Aufwärmaufgaben

Aufgabe 25.1. Zeige, dass der Quotient

$$\frac{1-x_3}{x_1+x_2 i}$$

für $x_1, x_2 \to 0$ und $x_3 = \pm\sqrt{1-x_1^2-x_2^2}$ gegen 0 konvergiert.

Aufgabe 25.2. Sei K ein algebraisch abgeschlossener Körper und sei $F \in K[X,Y]$ ein homogenes Polynom. Zeige: F zerfällt in Linearfaktoren.

Der in der Vorlesung verwendete Begriff einer Singularität wird durch folgende Definition präzisiert (es ist eher ein wichtiges Kriterium).

Es sei K ein algebraisch abgeschlossener Körper und seien $F_1, \ldots, F_s \in K[X_1, \ldots, X_n]$ Polynome mit der zugehörigen affinen Varietät

$$Y = V(F_1, \ldots, F_s) \subseteq \mathbb{A}_K^n,$$

die irreduzibel sei und die Dimension d besitze. Es sei $P \in Y$ ein abgeschlossener Punkt. Dann heißt P ein *glatter Punkt* von Y, wenn der Rang der Matrix

$$\left(\frac{\partial F_i}{\partial X_j}\right)_{i,j}$$

mindestens $n-d$ ist. Andernfalls heißt der Punkt *singulär*.

Die meisten Punkte einer affinen Varietät sind glatt, die singulären Punkte, wenn es sie denn gibt, bilden eine abgeschlossene Teilmenge, die der *singuläre Ort* von Y heißt. Die Varietät heißt *glatt*, wenn sie in jedem Punkt glatt ist.

Aufgabe 25.3. Zeige, dass der affine Raum $\mathbb{A}_K^n$ über einem algebraisch abgeschlossenen Körper K glatt ist.

Aufgabe 25.4. Zeige, dass die Ringe $K[X,Y,Z]/(XY-Z^n)$ (mit $n \geq 2$) genau in $P = (0,0,0)$ singulär sind.

Aufgabe 25.5. Zeige, dass die Ringe $K[X,Y,Z]/(X^2+YZ^2+Y^{m+1})$ (mit $m \geq 1$) genau in $P=(0,0,0)$ singulär sind.

Aufgabe 25.6. Zeige, dass der Ring $K[X,Y,Z]/(X^2+Y^3+Z^4)$ genau in $P=(0,0,0)$ singulär ist.

Aufgabe 25.7. Bestimme den singulären Ort von $K[X,Y,Z]/(X^2+YZ^2)$.

Aufgabe 25.8. Bestimme den singulären Ort von $K[X,Y,Z]/(X^2+YZ^2+Z^n)$.

Aufgabe 25.9. Zeige explizit, dass der Ring $\mathbb{C}[X,Y,Z]/(X^2+YZ^2+Y^2)$ (also die Diedersingularität zu $m=1$) isomorph zu $\mathbb{C}[S,T,U]/(ST-U^4)$ ist.

Aufgaben zum Abgeben

Aufgabe 25.10. (10 Punkte)

Bestimme zu den endlichen Untergruppen $G \subseteq \mathrm{SU}_2(\mathbb{C})$ die Halbachsenklassen auf S^2 und auf der projektiven Geraden $\mathbb{P}^1_{\mathbb{C}}$.

Aufgabe 25.11. (10 Punkte)

Bestimme zu den endlichen Untergruppen $G \subseteq \mathrm{SU}_2(\mathbb{C})$ und zu jeder Halbachsenklasse ein zugehöriges semiinvariantes Polynom.

26. Vorlesung - ADE Singularitäten

Die Invarianten der binären Oktaedergruppe

Wir setzen die Berechnung der Invariantenringe zu den Operationen der endlichen Untergruppen der $\mathrm{SU}_2(\mathbb{C})$ fort.

Beispiel 26.1. Zur Berechnung des Invariantenringes zur Operation der binären Oktaedergruppe BO auf $\mathbb{C}[U,V]$ benutzen wir die Normalteilerbeziehung BT $\subseteq$ BO (mit der Restklassengruppe $\mathbb{Z}/(2)$), Proposition 5.1 und Beispiel 25.5. Das Element $\begin{pmatrix} \xi & 0 \\ 0 & \xi^7 \end{pmatrix} \in \mathrm{BO} \setminus \mathrm{BT}$, wobei ξ eine achte primitive Einheitswurzel ist, wirkt durch $U \mapsto \xi U$ und $V \mapsto \xi^7 V$. Somit wird in der Darstellung

$$\mathbb{C}[U,V]^{\mathrm{BT}} = \mathbb{C}[N,P,Q]/(Q^2-P^3+108N^4)$$

das Polynom $N = UV(U^4 - V^4)$ auf

$$UV\left(-U^4 + V^4\right) = -N,$$

P auf P und Q auf $-Q$ geschickt. Auf dem isomorphen Ring $\mathbb{C}[X,Y,Z]/(X^2+Y^3+Z^4)$ ist dies einfach die Operation, die Y auf sich und X, Z auf ihr Negatives abbildet. Wir arbeiten mit der $\mathbb{Z}/(2)$-Graduierung, bei der Y den Grad 0 und X, Z den Grad 1 besitzen. Nach Korollar 7.11 ist der Invariantenring gleich der neutralen Stufe in der Graduierung. Diese Stufe wird neben Y von $R = XZ$ und $S = Z^2$ erzeugt (wegen $X^2 = -Y^3 - (Z^2)^2$ kann man auf X^2 verzichten). Zwischen Y, R, S besteht die Relation

$$R^2 + Y^3S + S^3 = (XZ)^2 + Y^3Z^2 + Z^6 = Z^2\left(X^2 + Y^3 + Z^4\right) = 0.$$

Nach Umbenennung der Variablen ist also der Invariantenring zur binären Oktaedergruppe isomorph zu

$$\mathbb{C}[X,Y,Z]/\left(X^2 + Y^3 + YZ^3\right).$$

Diesen Invariantenring bezeichnet man als *E_7-Singularität*.

Die Invarianten der binären Ikosaedergruppe

Der Invariantenring zur binären Ikosaedergruppe verhält sich in vielerlei Hinsicht anders als die bisher besprochenen Invariantenringe. Wir können den Invariantenring nicht aus der Kenntnis von anderen Invariantenringen berechnen. Dafür können wir zeigen, dass es keinen nichttrivialen Charakter der binären Ikosaedergruppe gibt, woraus sich über Satz 25.3 direkt invariante Polynome ergeben.

Lemma 26.2. *Die binäre Ikosaedergruppe* BI *besitzt keinen nichttrivialen Charakter.*

Beweis. Wir gehen von der Darstellung der binären Ikosaedergruppe in Beispiel 23.5 aus. Es sei

$$\psi\colon\ \mathrm{BI} \longrightarrow \mathbb{Z}/(\ell)$$

ein surjektiver Gruppenhomomorphismus. Wenn das Element $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ auf 0 abgebildet wird, so faktorisiert dieser Homomorphismus durch die reelle Ikosaedergruppe. Diese ist aber isomorph zur alternierenden Gruppe A_5, welche einfach ist. Also wird diese Matrix nicht auf 0 abgebildet und somit muss ℓ gerade ≥ 2 sein. Dann gibt es auch einen surjektiven Homomorphismus für $\ell = 2$. Der Kern dieser Abbildung besitzt 60 Elemente. Aufgrund der Liste in Satz 24.4 kommen dafür nur eine zyklische Gruppe oder eine Diedergruppe in Frage. In beiden Fällen hätte BI ein Element der Ordnung 15 und damit hätte auch die reelle Ikosaedergruppe ein solches Element, was aber nicht der Fall ist. □

Lemma 26.3. *Der Invariantenring $\mathbb{C}[U,V]^{BI}$ zur binären Ikosaedergruppe besitzt im Grad 60 die Dimension 2.*

Beweis. Wir verwenden Lemma 19.6 und Techniken, die auch im Beweis zur Formel von Molien verwendet werden. Sei dazu $\sigma \in BI$, das bezüglich einer geeigneten Basis durch eine Diagonalmatrix $\begin{pmatrix} \xi & 0 \\ 0 & \xi^{-1} \end{pmatrix}$ beschrieben wird, wobei ξ eine Einheitswurzel ist. Die Wirkungsweise dieses Elementes auf der d-ten Stufe $\mathbb{C}[W,Z]_d$ ist durch

$$W^i Z^{d-i} \mapsto \xi^i \xi^{i-d} W^i Z^{d-i} = \xi^{2i-d} W^i Z^{d-i}$$

gegeben (W, Z seien die Linearformen zur gewählten Basis). Daher ist die Spur von $\sigma^{(d)}$ durch

$$\sum_{i=0}^{d} \xi^{2i-d} \;=\; \xi^{-d} \sum_{i=0}^{d} \left(\xi^2\right)^i$$

gegeben. Sei nun $d = 60$. Da die Ordnung von σ nach Aufgabe 24.15 ein Teiler von 60 ist, sind die ξ, ξ^{-1}, ξ^2 sechzigste Einheitswurzeln. Bei $\sigma = \pm E_2$ ist diese Summe jeweils 61. Bei jedem anderen Gruppenelement ist nach Satz 24.3 $\xi^2 \neq 1$ und daher durchlaufen die Summanden von $i = 0$ bis $i = 59$ mehrfach sämtliche Potenzen von ξ^2, so dass diese Summe 0 ist und lediglich der Summand $(\xi^2)^{60} = 1$ übrigbleibt. Die Summe der Spuren zu allen $\sigma^{(60)}$, $\sigma \in BI$, ist somit $61 + 61 + 118 = 240$. Nach Lemma 19.6 ist also $\dim\left(\mathbb{C}[U,V]_{60}^{BI}\right) = 2$. □

Beispiel 26.4. Mit Hilfe von Satz 25.3 und Lemma 26.2 kann man direkt invariante Polynome für die binäre Ikosaedergruppe angeben. Ein Ikosaeder hat 12 Ecken, 20 Flächen und 30 Kanten, wobei die Ecken, die Flächenmittelpunkte und die Kantenmittelpunkte die Halbachsenklassen bilden. Daher gibt es invariante Polynome A, B, C vom Grad $12, 20$ und 30. Diese kann man mit einigem Rechenaufwand explizit ausrechnen, indem man explizit die Halbachsenklassen der reellen Ikosaedergruppe angibt (also beispielsweise alle zwölf Eckpunkte), diese ins Komplexe übersetzt und die zugehörigen Linearformen multipliziert. Unabhängig davon, ob diese Polynome explizit oder nicht vorliegen, kann man zeigen, dass diese den Invarianenring erzeugen, dass also $R^G = \mathbb{C}[A,B,C]$ gilt. Sei dazu $P \in R^G$ invariant, das wir als homogen annehmen dürfen. Wir führen Induktion über den Grad, wobei der Grad 0 der (triviale) Induktionsbeginn ist. Es sei P homogen von positivem Grad und es sei

$$P \;=\; \prod_{j=1}^{s} (d_j U - c_j V)$$

die Faktorzerlegung in Linearfaktoren. Nach Satz 25.3 (3) enthält die (nichtleere) Indexmenge eine volle Bahn der Operation der reellen Ikosaedergruppe auf S^2 bzw. $\mathbb{P}^1_{\mathbb{C}}$. Wenn diese Bahn eine Halbachsenklasse ist, so ist

$$P \;=\; HD$$

mit $D = A, B$ oder $= C$. Wegen der Invarianz von P und D ist auch H invariant. Nach Induktionsvoraussetzung ist also $H \in \mathbb{C}[A, B, C]$. Wenn dagegen die Indexmenge keine Halbachsenklasse enthält, so enthält sie eine Bahn mit sechzig Elementen (aus $\sigma(P) = P$ für $\sigma \in I$ folgt, dass P ein Halbachsenpunkt ist). Also ist

$$P = HD$$

und D ist invariant vom Grad 60. Nach Lemma 26.3 ist der Raum der invarianten Polynome vom Grad 60 zweidimensional. Die Polynome A^5, B^3, C^2 erzeugen diesen Raum, da sie paarweise linear unabhängig sind, was daraus folgt, dass sie (in $\mathbb{C}[U, V]$) aus unterschiedlichen Linearfaktoren zusammengesetzt sind. Daher ist $D \in \mathbb{C}[A, B, C]$ und dies gilt nach Induktionsvoraussetzung auch für H.

Weiterhin folgt aus der Zweidimensionalität der sechzigsten Stufe des Invariantenringes, dass eine Relation der Form

$$\alpha A^5 + \beta B^3 + \gamma C^2 = 0$$

mit $\alpha, \beta, \gamma \neq 0$ vorliegen muss, was den Isomorphietyp des Ringes bereits bestimmt.

Wir geben noch die invarianten Polynome zu den Halbachsen an, und zwar geben wir homogene invariante Polynome vom Grad $12, 20, 30$ an, wobei wir die Invarianz nur exemplarisch überprüfen. Wir setzen

$$\tilde{A} = U^{11}V + 11U^6V^6 - UV^{11},$$
$$\tilde{B} = U^{20} - 228U^{15}V^5 + 494U^{10}V^{10} - 228U^5V^{15} + V^{20}$$

und

$$\tilde{C} = U^{30} + 522U^{25}V^5 - 10005U^{20}V^{10} - 10005U^{10}V^{20} + 522U^5V^{25} + V^{30}.$$

Wenn man nachweist, dass diese Polynome invariant sind, so muss wegen $\tilde{A}, \tilde{B}, \tilde{C} \in \mathbb{C}[A, B, C]$ und aus Gradgründen (bis auf Skalierung) $\tilde{A} = A$, $\tilde{B} = B$ und $\tilde{C} = C$ gelten. Die erzeugenden Matrizen

$$E = -\begin{pmatrix} \xi^3 & 0 \\ 0 & \xi^2 \end{pmatrix} \text{ und } F = \frac{1}{\sqrt{5}}\begin{pmatrix} -\xi + \xi^4 & \xi^2 - \xi^3 \\ \xi^2 - \xi^3 & \xi - \xi^4 \end{pmatrix}$$

(wobei ξ eine primitive 5-te komplexe Einheitswurzel sei) der binären Ikosaedergruppe wirken durch

$$U \mapsto -\xi^3 U,\ V \mapsto -\xi^2 V$$

bzw.

$$U \mapsto \frac{1}{\sqrt{5}}\left((-\xi + \xi^4)U + (\xi^2 - \xi^3)V\right),\ V \mapsto \frac{1}{\sqrt{5}}\left((\xi^2 - \xi^3)U + (\xi - \xi^4)V\right).$$

Es ist

$$\begin{aligned} (\tilde{A})E &= (U^{11}V + 11U^6V^6 - UV^{11})E \\ &= (-\xi^{33})(-\xi^2)U^{11}V + 11(\xi^{18}\xi^{12})U^6V^6 - (-\xi^3)(-\xi^{22})UV^{11} \\ &= U^{11}V + 11U^6V^6 - UV^{11} \end{aligned}$$

und (mit einer aufwändigen Rechnung)

$$\begin{aligned}(\tilde{A})F &= (U^{11}V + 11U^6V^6 - UV^{11})F \\ &= U^{11}V + 11U^6V^6 - UV^{11}.\end{aligned}$$

Zwischen diesen invarianten Polynomen besteht, wie eine aufwändige Rechnung zeigt, die Beziehung

$$\begin{aligned}\tilde{C}^2 - \tilde{B}^3 - 1728\tilde{A}^5 &= \left(U^{30} + 522U^{25}V^5 - 10005U^{20}V^{10} - 10005U^{10}V^{20} + 522U^5V^{25} + V^{30}\right)^2 \\ &\quad - \left(U^{20} - 228U^{15}V^5 + 494U^{10}V^{10} - 228U^5V^{15} + V^{20}\right)^3 \\ &\quad -1728\left(U^{11}V + 11U^6V^6 - UV^{11}\right)^5 \\ &= U^{55}V^5\left(1044 + 684 - 1728\right) + \ldots = 0.\end{aligned}$$

Dies überprüft man, indem man die Koeffizienten zu den Monomen $U^{5i}V^{5j}$, $i + j = 12$, berechnet. Da diese Relation irreduzibel ist, liegt die Isomorphie

$$\mathbb{C}[U,V]^{BI} = \mathbb{C}[\tilde{A},\tilde{B},\tilde{C}]/(\tilde{C}^2 - \tilde{B}^3 - 1728\tilde{A}^5)$$

vor. Nach Umbenennung und Streckung der Variablen ist dieser Ring isomorph zu $\mathbb{C}[X,Y,Z]/(X^2 + Y^3 + Z^5)$.

Diesen Invariantenring bezeichnet man als E_8-*Singularität*.

Satz 26.5. *Der Restklassenring* $\mathbb{C}[X,Y,Z]/(X^2 + Y^3 + Z^5)$ *ist faktoriell.*

Beweis. Dies folgt aus Lemma 26.2, Beispiel 26.4 und Korollar 12.9. □

Bemerkung 26.6. Die Komplettierung des Ringes $R = \mathbb{C}[X,Y,Z]/(X^2 + Y^3 + Z^5)$ am maximalen Ideal R_+ ist $\hat{R} = \mathbb{C}[[X,Y,Z]]/(X^2 + Y^3 + Z^5)$. Dieser Ring ist ebenfalls faktoriell (die Komplettierung eines faktoriellen Ringes muss im Allgemeinen nicht faktoriell sein). Es gilt sogar, dass dieser Ring der einzige zweidimensionale komplette Ring (bis auf Isomorphie) über $\mathbb{C}$ ist, der faktoriell, aber nicht regulär, also nicht der Potenzreihenring $\mathbb{C}[[X,Y]]$ ist.

26. Arbeitsblatt

Aufwärmaufgaben

Aufgabe 26.1. Zeige, dass der Ring $K[X,Y,Z]/(X^2 + Y^3 + YZ^3)$ genau in $P = (0,0,0)$ singulär ist.

Aufgabe 26.2. Bestimme für die binäre Tetraedergruppe die Dimension von $\mathbb{C}[U,V]_d^{BT}$ für $d \leq 12$.

Aufgabe 26.3. Bestimme für die binäre Oktaedergruppe die Dimension von $\mathbb{C}[U,V]_d^{BO}$ für $d \leq 24$.

Aufgabe 26.4. Zeige, dass der Ring $K[X,Y,Z]/(X^2+Y^3+Z^5)$ genau in $P=(0,0,0)$ singulär ist.

Aufgabe 26.5. Zeige, dass es auf den A- und den D-Singularitäten und auf der E_6 und der E_7-Singularität glatte Kurven gibt, die durch den singulären Punkt laufen.

Aufgabe 26.6. Bestätige, dass die in Beispiel 26.4 angegebenen Polynome $\tilde{A},\tilde{B},\tilde{C}$ in der Tat invariant sind, und dass die dort angegebene Relation besteht.

Aufgabe 26.7. Zeige, dass es einen injektiven Ringhomomorphismus

$$\mathbb{C}[X,Y,Z]/(X^2+Y^3+Z^5) \longrightarrow \mathbb{C}[R,S,T]/(RS-T^2)$$

gibt.

Aufgabe 26.8. Zeige, dass die Ringe der ADE-Singularitäten eine positive Graduierung besitzen. Man gebe diese jeweils an.

Wir erinnern an folgende Definition.

Zu einer Gruppe G heißt die von allen Kommutatoren $aba^{-1}b^{-1}$, $a,b \in G$, erzeugte Untergruppe die *Kommutatorgruppe* von G. Sie wird mit $K(G)$ bezeichnet.

Die Kommutatorgruppe ist nach Lemma 20.5 (Körper- und Galoistheorie (Osnabrück 2011)) ein Normalteiler, die Restklassengruppe $G/K(G)$ nennt man auch die *Abelianisierung* von G.

Aufgabe 26.9. Bestimme zu den endlichen Untergruppen $G \subseteq \mathrm{SU}_2(\mathbb{C})$ jeweils die Kommutatoruntergruppe und die Abelianisierung.

Aufgaben zum Abgeben

Aufgabe 26.10. (4 Punkte)

Zeige, dass es auf der E_8-Singularität keine glatte Kurve gibt, die durch den singulären Punkt läuft.

27. Vorlesung - Lokale Fundamentalgruppe

Zu einer endlichen Untergruppe $G \subseteq \mathrm{SU}_2(\mathbb{C})$ liegt im Quotienten $X = \mathbb{C}^2 \backslash G$ im Bildpunkt P von $0 \in \mathbb{C}^2$ eine Singularität vor, dagegen ist $X \setminus \{P\}$ glatt. Wir stellen uns die folgenden Fragen:

Kann man es dieser glatten offenen Menge ansehen, dass sie nur durch einen singulären Punkt zu einer affinen Varietät abgeschlossen wird (oder könnte man sie auch durch einen glatten Punkt abschließen)?

Kann man die Gruppe G, mit der wir X definiert haben, aus intrinsischen Eigenschaften von X oder von $X \setminus \{P\}$ rekonstruieren?

Sind die zu den unterschiedlichen G auftretenden Quotienten untereinander verschieden?

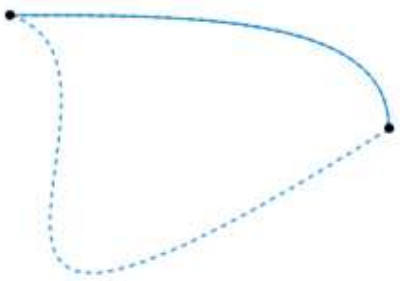
Wir werden all diese Fragen positiv beantworten, wobei wir eine wichtige topologische Konstruktion einsetzen, nämlich die Fundamentalgruppe.

Die Fundamentalgruppe

Es sei X ein topologischer Raum, den wir als wegzusammenhängend voraussetzen wollen, zu je zwei Punkten $x, y \in X$ gibt es also einen stetigen Weg

$$\gamma\colon\ [0,1] \longrightarrow X$$

mit $\gamma(0) = x$ und $\gamma(1) = y$.



Zwei Wege

$$\gamma_0, \gamma_1\colon\ [0,1] \longrightarrow X$$

heißen *homotop*, wenn es eine stetige Abbildung (die eine *Homotopie* zwischen γ_0 und γ_1 genannt wird)

$$\Gamma\colon\ [0,1] \times [0,1] \longrightarrow X$$

gibt, für die

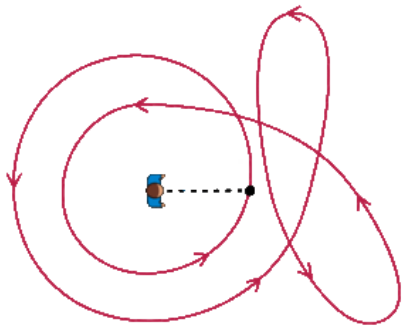
$$\Gamma(s,0) = \gamma_0(s),\ \Gamma(s,1) = \gamma_0(s),\ \Gamma(0,t) = x \text{ und } \Gamma(1,t) = y$$

für alle s, t gilt. Zu jedem festen t ist $\Gamma(-, t)$ ein stetiger Weg von x nach y. Die Homotopie ist eine Äquivalenzrelation auf der Menge der stetigen Wege von x nach y. Ein Weg γ heißt *geschlossen*, wenn $\gamma(0) = \gamma(1)$ ist, wenn also der Startpunkt mit dem Endpunkt übereinstimmt. Dieser Punkt heißt dann auch *Aufpunkt* des Weges. Häufig betrachtet man stetige geschlossene Wege in X als stetige Abbildungen $\gamma\colon\ S^1 \to X$.

Zwei stetige geschlossene Wege kann man miteinander verknüpfen, indem man zuerst den einen Weg und anschließend den anderen Weg durchläuft. Als Definitionsbereich erhält man dabei das Intervall $[0, 2]$. Man kann aber, indem man die beiden Wege doppelt so schnell durchläuft, auch das Einheitsintervall als Definitionsbereich wählen. Wichtig ist, dass zu geschlossenen homotopen Wegen $\gamma_0 \sim \delta_0$ und $\gamma_1 \sim \delta_1$ auch die Verknüpfungen $\gamma = \gamma_0\gamma_1$ und $\delta = \delta_0\delta_1$ homotop sind. Dies erlaubt eine Verknüpfung auf der Menge der Äquivalenzklassen von homotopen geschlossenen Wegen mit Aufpunkt x, die mit $\pi_1(X, x)$ bezeichnet wird. Diese Menge ist mit dem konstanten Weg (also der Homotopieklasse des konstanten Weges) als neutralem Element eine Gruppe, die die *Fundamentalgruppe* von X heißt. Die Assoziativität ist dabei nicht völlig selbstverständlich, da drei geschlossene Weg je nach Klammerung zu unterschiedlichen Wegen auf dem Einheitsintervall führen. Die enstehenden Wege sind aber homotop, so dass auf den Homotopieklassen die Assoziativität gilt. Die inverse Homotopieklasse ist durch den entgegengesetzt durchlaufenen Weg gegeben. Deren Verknüpfung ist in der Tat homotop zum konstanten Weg, oder, wie man auch sagt, *nullhomotop*.

Definition 27.1. Ein topologischer Raum X heißt *einfach-zusammenhängend*, wenn er wegzusammenhängend ist und wenn jeder stetige geschlossene Weg in X nullhomotop ist.

Der einfache Zusammenhang bedeutet, dass $\pi_1(X, x) = 0$ ist (für einen beliebigen Aufpunkt $x \in X$).



Die Fundamentalgruppe der punktierten reellen Ebene ist $\mathbb{Z}$, man spricht von der *Windungszahl* des Weges.

Definition 27.2. Ein topologischer Raum X heißt *kontrahierbar* (oder *zusammenziehbar*) auf einen Punkt $P \in X$, wenn es eine stetige Abbildung

$$H\colon\ [0,1] \times X \longrightarrow X$$

gibt derart, dass die Eigenschaften

(1) $H(1,-) = \mathrm{Id}_X$,
(2) $H(0,-) = P$,
(3) $H(t,P) = P$ für alle $t \in [0,1]$

gelten.

Beispielsweise ist der $\mathbb{R}^n$ kontrahierbar und nach dem folgenden Satz auch einfach zusammenhängend.

Satz 27.3. *Die Fundamentalgruppe eines kontrahierbaren Raumes ist trivial.*

Zu einer stetigen Abbildung

$$\varphi\colon\ X \longrightarrow Y$$

und einem Punkt $x \in X$ mit $y = \varphi(x)$ induziert ein stetiger geschlossener Weg $\gamma\colon\ [0,1] \to X$ mit Aufpunkt x einen stetigen geschlossenen Weg $\varphi \circ \gamma$ in Y mit Aufpunkt y. Diese Zuordnung ist mit Homotopien von Wegen verträglich, d.h. wenn $\gamma \sim \delta$ zwei homotope Wege in X mit Aufpunkt x sind, so sind auch $\varphi \circ \gamma$ und $\varphi \circ \delta$ homotop. Daher gibt es eine wohldefinierte Abbildung

$$\pi_1(X,x) \longrightarrow \pi_1(Y,y).$$

Diese Abbildung ist sogar ein Gruppenhomomorphismus.

Die Berechnung der Fundamentalgruppe ist im Allgemeinen schwierig. Ein wichtiges Hilfsmittel sind Überlagerungen.

Definition 27.4. Es seien X und Y topologische Räume. Eine stetige Abbildung

$$p\colon\ Y \longrightarrow X$$

heißt *Überlagerung*, wenn es eine offene Überdeckung $X = \bigcup_{i\in I} U_i$ und eine Familie diskreter topologischer Räume F_i, $i \in I$, derart gibt, dass $p^{-1}(U_i)$ homöomorph zu $U_i \times F_i$ (versehen mit der Produkttopologie) ist, wobei die Homöomorphien mit den Abbildungen nach U_i verträglich sind.

Zu einer stetigen Abbildung $\pi\colon\ Y \to X$ und einem stetigen Weg

$$\gamma\colon\ [0,1] \longrightarrow X$$

nennt man einen stetigen Weg

$$\tilde{\gamma}\colon\ [0,1] \longrightarrow Y$$

mit

$$\gamma\ =\ \pi \circ \tilde{\gamma}$$

eine *Liftung* von γ. Bei einem geschlossenen Weg verlangt man dabei *nicht*, dass die Liftung wieder geschlossen ist. Zu einer Überlagerung und einem vorgegebenen Punkt $y \in Y$ über $\gamma(0)$ gibt es eine eindeutige Liftung $\tilde{\gamma}$ mit

$$\tilde{\gamma}(0) = y.$$

Zur Fundamentalgruppe der Quotientensingularitäten

Sei $X = \mathbb{C}^2 \backslash G = \left(\operatorname{Spek}\left(\mathbb{C}[U,V]\right)^G\right)_{\mathbb{C}}$. Wir wollen zeigen, dass man die operierende Gruppe G im Quotienten X wiederfinden kann, und zwar als Fundamentalgruppe der punktierten Singularität, also des Quotienten ohne den singulären Punkt.

Zuerst zeigen wir, dass die Fundamentalgruppe (des Spektrums) einer positiv-graduierten Algebra trivial ist.

Lemma 27.5. *Es sei R eine positiv-graduierte endlich-erzeugte $\mathbb{C}$-Algebra. Dann ist $X = (\operatorname{Spek}(R))_{\mathbb{C}}$ kontrahierbar und die Fundamentalgruppe $\pi_1(X)$ ist trivial.*

Beweis. Es ist $X \subseteq \mathbb{C}^n$ eine abgeschlossene Teilmenge, die unter der Operation

$$\mathbb{C}^\times \times \mathbb{C}^n \longrightarrow \mathbb{C}^n$$

mit

$$t(x_1, \ldots, x_n) = (t^{d_1}x_1, \ldots, t^{d_n}x_n)$$

von $t \in \mathbb{C}^\times$ abgeschlossen ist, wobei die d_i die positiven Grade der Erzeuger der Algebra bezeichnen. Es genügt daher, eine Kontraktion des affinen Raumes $\mathbb{C}^n$ auf den Nullpunkt anzugeben, die mit den Bahnen der Operation verträglich ist. Dazu setzen wir die Operationsabbildung zu einer Abbildung

$$\mathbb{C} \times \mathbb{C}^n \longrightarrow \mathbb{C}^n$$

mit der gleichen Vorschrift fort. Wegen $d_i \geq 1$ ist dies wohldefiniert und algebraisch, also insbesondere stetig. Für $t = 0$ ist dies die Nullabbildung und für $t = 1$ die Identität. Für jedes $t \in [0,1]$ wird der Nullpunkt auf sich abgebildet. Die auf die Verbindungsstrecke von 0 nach 1 eingeschränkte Abbildung

$$[0,1] \times \mathbb{C}^n \longrightarrow \mathbb{C}^n$$

ist somit eine kontrahierende Abbildung auf den Nullpunkt. Nach Satz 27.3 ist die Fundamentalgruppe trivial. □

Zu einer endlich erzeugten zusammenhängenden $\mathbb{C}$-Algebra R, einem maximalen Ideal $\mathfrak{m} \subseteq R$ und dem zugehörigen Punkt $P \in X = (\operatorname{Spek}(R))_{\mathbb{C}}$ nennt man die Fundamentalgruppe von $X \setminus \{P\}$ die lokale Fundamentalgruppe von X in P. Bei einer positiv graduierten $\mathbb{C}$-Algebra meint man mit der lokalen Fundamentalgruppe die lokale Fundamentalgruppe im Punkt, der zum irrelevanten Ideal R_+ gehört.

Im Fall der ADE-Singularitäten ist $(0,0) \in \mathbb{C}^2$ der Fixpunkt der Gruppenoperation und sein Bildpunkt im Quotienten ist der singuläre Punkt $P \in X$. Wenn man die beiden Punkte $(0,0)$ und P herausnimmt, so erhält man eine Gruppenoperation von G auf $\mathbb{C}^2 \setminus \{(0,0)\}$ mit dem Quotienten $X \setminus \{P\}$. Wir werden gleich begründen, dass die Abbildung

$$\mathbb{C}^2 \setminus \{(0,0)\} \longrightarrow X \setminus \{P\}$$

eine Überlagerung ist und dass die Fundamentalgruppe von $X \setminus \{P\}$ isomorph zu G ist. Dazu zitieren wir ohne Beweis den folgenden Satz.

Satz 27.6. *Es sei G eine endliche Gruppe, die auf einem einfach zusammenhängenden Hausdorff-Raum X fixpunktfrei operiere. Dann ist*

$$X \longrightarrow X \backslash G$$

eine Überlagerung und die Fundamentalgruppe des Bahnenraumes $X \backslash G$ ist gleich G.

Satz 27.7. *Es sei $G \subseteq \mathrm{SL}_2(\mathbb{C})$ eine endliche Untergruppe mit der zugehörigen zweidimensionalen speziellen Quotientensingularität $R = \mathbb{C}[U,V]^G$. Dann gelten folgende Aussagen.*

(1) *Die Operation von G auf $\mathbb{C}^2 \setminus \{(0,0)\}$ ist fixpunktfrei.*
(2) *Die lokale Fundamentalgruppe von $(\mathrm{Spek}\,(R))_{\mathbb{C}} \setminus \{P\}$ ist gleich G, wobei P der singuläre Punkt von $(\mathrm{Spek}\,(R))_{\mathbb{C}}$ ist.*

Beweis. (1). Die zu $\sigma \in G$ gehörende lineare Abbildung besitze einen Fixpunkt $\neq 0$. Dann ist dies ein Eigenvektor zum Eigenwert 1. Da σ nach Satz 3.19 diagonalisierbar ist, ist in einer geeigneten Basis

$$\sigma = \begin{pmatrix} 1 & 0 \\ 0 & \zeta \end{pmatrix}$$

und wegen $G \subseteq \mathrm{SL}_2(\mathbb{C})$ ist $\zeta = 1$, also ist σ die Identität. (2) folgt aus (1) und Satz 27.6, unter Berücksichtigung von Aufgabe 15.11 und Aufgabe 27.10. □

Dies beantwortet die eingangs erwähnten Fragen positiv. Für die erste Frage muss man wissen, dass eine komplex-zweidimensionale affine glatte Varietät, in jedem ihrer Punkte eine triviale lokale Fundamentalgruppe besitzt, da eine offene Umgebung des glatten Punktes diffeomorph zu einem offenen Ball im $\mathbb{C}^2 \cong \mathbb{R}^4$ ist und ein solcher punktierter Ball eine triviale Fundamentalgruppe besitzt.

27. Arbeitsblatt

Aufwärmaufgaben

Aufgabe 27.1. Es sei X ein topologischer Raum und $x, y \in X$. Zeige, dass die Homotopie von Wegen eine Äquivalenzrelation auf der Menge der stetigen Wege von x nach y ist.

Aufgabe 27.2. Es sei X ein topologischer Raum. Zeige, dass die Verknüpfung von stetigen Wegen

$$\gamma, \delta \colon [0,1] \longrightarrow X$$

durch Hintereinanderausführung zu einer wohldefinierten Verknüpfung auf den Homotopieklassen von Wegen führt.

Aufgabe 27.3. Es sei X ein topologischer Raum und $x \in X$. Zeige, dass die Verknüpfung eines stetigen geschlossenen Weges γ mit Aufpunkt x mit dem konstanten Weg x homotop zu γ ist.

Aufgabe 27.4. Es sei X ein topologischer Raum und $x, y \in X$. Es sei

$$\gamma \colon [0,1] \longrightarrow X$$

ein stetiger Weg von x nach y und sei γ^{-1} der umgekehrt durchlaufene Weg, also $\gamma^{-1}(t) := \gamma(1-t)$. Zeige, dass die Verknüpfung $\gamma\gamma^{-1}$ homotop zum konstanten Weg x ist.

Aufgabe 27.5. Es sei X ein topologischer Raum und $x \in X$. Zeige, dass die Verknüpfung von Homotopieklassen geschlossener Wege mit Aufpunkt x assoziativ ist.

Aufgabe 27.6. Es sei X ein topologischer Raum und

$$\gamma \colon S^1 \longrightarrow X$$

ein stetiger geschlossener Weg. Zeige, dass γ genau dann nullhomotop ist, wenn es eine stetige Fortsetzung von γ auf die abgeschlossene Kreisscheibe gibt.

Aufgabe 27.7. Zeige, dass der $\mathbb{R}^n$ kontrahierbar ist.

Aufgabe 27.8. Es sei $\varphi\colon X \to Y$ eine stetige Abbildung zwischen topologischen Räumen und $x \in X$ mit $\varphi(x) = y$. Zeige, dass die Zuordnung

$$\gamma \mapsto \varphi \circ \gamma$$

eine wohldefinierte Abbildung auf der Menge der Homotopieklassen geschlossener Wege (mit Aufpunkt x bzw. y) induziert.

Aufgabe 27.9. Es sei $\varphi\colon X \to Y$ eine stetige Abbildung zwischen topologischen Räumen und $x \in X$ mit $\varphi(x) = y$. Zeige, dass die Zuordnung

$$\gamma \mapsto \varphi \circ \gamma$$

zu einem Gruppenhomomorphismus

$$\pi_1(X,x) \longrightarrow \pi_1(Y,y)$$

führt.

Aufgabe 27.10. Zeige, dass bei $n \geq 3$ der $\mathbb{R}^n \setminus \{P\}$ einfach zusammenhängend ist.

Aufgabe 27.11. Es sei

$$\mathbb{Z} \longrightarrow \mathbb{Z}$$

ein Gruppenhomomorphismus und

$$\varphi\colon \mathbb{C}^\times \cong \left(\operatorname{Spek}\left(\mathbb{C}[T,T^{-1}]\right)\right)_{\mathbb{C}} \longrightarrow \mathbb{C}^\times \cong \left(\operatorname{Spek}\left(\mathbb{C}[T,T^{-1}]\right)\right)_{\mathbb{C}}$$

die zugehörige Spektrumsabbildung zwischen den Spektra der Monoidringe. Wie sieht die zugehörige Abbildung der Fundamentalgruppen aus?

Aufgabe 27.12. Zeige, dass die Abbildung

$$\mathbb{R} \longrightarrow S^1,\, t \longmapsto (\cos t\,,\, \sin t\,),$$

eine Überlagerung ist.

Aufgabe 27.13. Zeige, dass die Abbildung

$$\mathbb{C} \longrightarrow \mathbb{C}^\times = \mathbb{C} \setminus \{0\},\, z \longmapsto \exp z,$$

eine Überlagerung ist.

Aufgaben zum Abgeben

Aufgabe 27.14. (3 Punkte)

Bestimme die Fundamentalgruppe des reell-projektiven Raumes $\mathbb{P}^n_{\mathbb{R}}$.

Aufgabe 27.15. (4 Punkte)

Es sei $R = \mathbb{C}[T_1, \ldots, T_n]/\mathfrak{a}$ eine endlich erzeugte positiv-graduierte $\mathbb{C}$-Algebra und $X = \mathbb{C}$–Spek $(R) \subseteq \mathbb{C}^n$ das $\mathbb{C}$-Spektrum von R. Es sei $S = \{z \in X | \ ||z|| = 1\}$ die „Sphäre“ von X (bezüglich der gegebenen Einbettung). Zeige, dass es eine Homotopie zwischen $X \setminus \{0\}$ und S gibt. Man folgere, dass die punktierte Fundamentalgruppe von R gleich der Fundamentalgruppe von S ist.

28. Vorlesung - Fundamentalgruppe von Monoidringen

Die lokale Fundamentalgruppe von Monoidringen

In der letzten Vorlesung haben wir gesehen, dass im Falle der ADE-Singularitäten die operierende Gruppe als lokale Fundamentalgruppe des Invariantenringens, also als Fundamentalgruppe des punktierten Quotientenraumes wiederkehrt. Die A-Singularitäten sind Monoidringe der Form $\mathbb{C}[X, Y, Z]/(XY - Z^n)$, die operierende Gruppe ist die zyklische Gruppe $\mathbb{Z}/(n)$ und dies ist auch die lokale Fundamentalgruppe. In dieser Vorlesung beschäftigen wir uns generell mit der lokalen Fundamentalgruppe von Monoidringen, wobei wir diese wieder wie in der neunten Vorlesung als Invariantenringe zu einer kommutativen Gruppe und als Ringe der neutralen Stufe einer Gradierung auf einem Polynomring auffassen.

Die Grundidee ist folgende: Wenn M ein Monoid ist und

$$\gamma\colon\ M \longrightarrow \mathbb{Z}$$

ein Monoidhomomorphismus, so induziert dies nach Korollar 8.6 einen $\mathbb{C}$-Algebrahomomorphismus

$$\mathbb{C}[M] \longrightarrow \mathbb{C}[\mathbb{Z}] \cong \mathbb{C}[T, T^{-1}]$$

und damit eine Spektrumsabbildung

$$\operatorname{Spek}\left(\mathbb{C}[T, T^{-1}]\right) \longrightarrow \operatorname{Spek}\left(\mathbb{C}[M]\right),$$

also einen Morphismus der punktierten Geraden in das Spektrum des Monidringes. In der natürlichen Topologie liegt somit eine stetige Abbildung

$$\mathbb{C}^\times \cong \left(\operatorname{Spek}\left(\mathbb{C}[T, T^{-1}]\right)\right)_{\mathbb{C}} \longrightarrow Y_{\mathbb{C}} = \left(\operatorname{Spek}\left(\mathbb{C}[M]\right)\right)_{\mathbb{C}}$$

vor. Durch Einschränken dieser Abbildung auf den Einheitskreis $S^1 \subseteq \mathbb{C}^\times$ erhält man eine stetige Abbildung des Kreises nach Y (bzw. in eine gewisse offene Teilmenge $U \subseteq Y$) und damit einen geschlossenen Weg. Es wird sich herausstellen, dass diese Wege, unter bestimmten Voraussetzungen, zur Berechnung der Fundamentalgruppe entscheidend sind.

Zur weiteren Durchführung dieser Idee sei das Monoid als

$$M \ = \ \ker \delta \cap \mathbb{N}^r$$

zu einem surjektiven Gruppenhomomorphismus (einer Graduierung)

$$\delta\colon\ \mathbb{Z}^r \longrightarrow D$$

gegeben. Dann ist $\mathbb{C}[M] \subseteq \mathbb{C}[X_1, \ldots, X_r]$ der Ring der neutralen Stufe in dieser Graduierung und nach Satz 9.5 der Invariantenring zur zugehörigen Operation der Charaktergruppe $D^\vee$ auf $\mathbb{A}^r_{\mathbb{C}}$. Die zugehörige Spektrumsabbildung

$$\mathbb{A}^r_{\mathbb{C}} \longrightarrow \operatorname{Spek}(\mathbb{C}[M])$$

induziert, wenn man sie auf geeignete offene Teilmengen einschränkt, in der natürlichen Topologie eine Überlagerung, mit deren Hilfe man in vielen Fällen (aber nicht ohne weitere Voraussetzungen) die lokale Fundamentalgruppe berechnen kann. Eine wichtige Voraussetzung ist, dass D endlich ist. Die Formulierung im folgenden Satz ist ziemlich aufwändig, vereinfacht sich aber wesentlich, wenn man an $r = 2$ und $T = \{(0,0)\}$ denkt.

Satz 28.1. *Es sei D eine kommutative endliche Gruppe und $\delta\colon\ \mathbb{Z}^r \to D$ ein surjektiver Gruppenhomomorphismus mit $r \geq 2$. Diesen Gruppenhomomorphismus fassen wir als D-Graduierung auf dem Polynomring $\mathbb{C}[X_1, \ldots, X_r]$ und als Operation der Charaktergruppe $G = D^\vee$ auf dem $\mathbb{C}^r$ auf. Es sei Γ der Kern von δ, $M = \Gamma \cap \mathbb{N}^r$ das zugehörige Monoid und*

$$\mathbb{C}[M] \subseteq \mathbb{C}[X_1, \ldots, X_r]$$

die zugehörige Inklusion des Monoidringes. Es sei

$$q\colon\ \mathbb{C}^r \longrightarrow Y = \operatorname{Spek}(\mathbb{C}[M])_{\mathbb{C}}$$

die zugehörige Quotientenabbildung. Es sei eine Zariski-abgeschlossene G-invariante Teilmenge $T \subset \mathbb{C}^r$ derart gegeben, dass T ganz in der Vereinigung der Achsenhyperebenen liegt, dass T mindestens die Kodimension 2 besitzt und dass die induzierte Operation von G auf $\mathbb{C}^r \setminus T$ fixpunktfrei sei. Dann gelten folgende Aussagen.

(1) *Die Fundamentalgruppe von*

$$Y \setminus q(T) \ = \ (\mathbb{C}^r \setminus T) \setminus G$$

ist G.

(2) *Es sei $m \in \mathbb{N}_+$ derart, dass*[9] *$m\mathbb{Z}^r \subseteq \Gamma$ ist. Die Zuordnung*

$$F\colon\ \operatorname{Hom}(\Gamma, \mathbb{Z}) \longrightarrow \operatorname{Hom}\left(\mathbb{Z}^r, \mathbb{C}^\times\right),\ \gamma \longmapsto F(\gamma) = \left(e_j \mapsto e^{\frac{2\pi i \gamma(me_j)}{m}}\right),$$

induziert einen Gruppenisomorphismus

$$\operatorname{Hom}(\Gamma, \mathbb{Z}) \,/\, \operatorname{bild}(\operatorname{Hom}(\mathbb{Z}^r, \mathbb{Z})) \longrightarrow G.$$

[9] Ein solches m gibt es stets.

(3) *Die zu* $\gamma \in \mathrm{Hom}\,(\Gamma, \mathbb{Z})$ *gehörende Abbildung*

$$\gamma^*\colon\ \mathbb{C}^\times \longrightarrow \left(\mathbb{C}^\times\right)^r \subseteq Y \setminus q(T),\ t \longmapsto (t^{\gamma(u_1)}, \ldots, t^{\gamma(u_r)}),$$

(u_j *sei eine Basis von* $\Gamma \cong \mathbb{Z}^r$*) ergibt durch Einschränkung auf* $S^1 \subseteq \mathbb{C}^\times$ *einen stetigen geschlossenen Weg*

$$[0, 2\pi] \longrightarrow Y \setminus q(T).$$

(4) *Die Liftung des Weges aus (3) nach* $\mathbb{C}^r \setminus T$ *mit dem Anfangspunkt* $(1Vorlage : Kommadots1)$ *ist durch*

$$[0, 2\pi] \longrightarrow \mathbb{C}^r \setminus T,\ s \longmapsto \left(e^{\frac{is\gamma(me_1)}{m}}, \ldots, e^{\frac{is\gamma(me_r)}{m}}\right),$$

gegeben. Der Weg $\gamma^*|_{S^1}$ *repräsentiert das nach (2) zu* γ *gehörende Element in der Fundamentalgruppe* G*.*

Beweis. (1) folgt aus Satz 27.6, da $\mathbb{C}^r \setminus T$ wegen der Bedingung an die Kodimension[10] einfach zusammenhängend und die Operation darauf nach Voraussetzung fixpunktfrei ist. (2). Die Abbildung F ist wegen der Funktionalgleichung der Exponentialfunktion ein Gruppenhomomorphismus. Die Abbildung $F(\gamma)$ ist auf der Untergruppe $\Gamma \subseteq \mathbb{Z}^r$ trivial. Für $u \in \Gamma$ ist ja $\gamma(mu) = m\gamma(u)$ und somit ist

$$e^{\frac{2\pi i\gamma(mu)}{m}} = e^{\frac{2\pi im\gamma(u)}{m}} = e^{2\pi i\gamma(u)} = 1.$$

Daher ist $F(\gamma)$ in natürlicher Weise ein Gruppenhomomorphismus

$$\mathbb{Z}^r/\Gamma \cong D \longrightarrow \mathbb{C}^\times,$$

also ein Charakter auf D. Zur Bestimmung des Kerns von F sei zunächst γ die Einschränkung eines Gruppenhomomorphismus

$$\tilde{\gamma}\colon\ \mathbb{Z}^r \longrightarrow \mathbb{Z}$$

auf $\Gamma \subseteq \mathbb{Z}^r$. Doch dann ist natürlich $\gamma(me_j) = m\tilde{\gamma}(e_j)$ für die Basis e_j von $\mathbb{Z}^r$ und somit ist der zugehörige Charakter trivial. Wenn umgekehrt der zugehörige Charakter trivial ist, so muss $\frac{\gamma(me_j)}{m} \in \mathbb{Z}$ für jedes e_j gelten. Doch dann ist durch

$$\tilde{\gamma}(e_j) := \frac{\gamma(me_j)}{m}$$

eine Fortsetzung von γ nach $\mathbb{Z}^r$ gegeben. Es liegt also ein injektiver Gruppenhomomorphismus

$$\mathrm{Hom}\,(\Gamma, \mathbb{Z}) \,/\, \mathrm{bild}\,(\mathrm{Hom}\,(\mathbb{Z}^r, \mathbb{Z})) \longrightarrow G$$

[10]Dies beruht auf dem Satz, dass bei einer reellen Mannigfaltigkeit M und einer abgeschlossenen Untermannigfaltigkeit $N \subseteq M$ der reellen Kodimension ≥ 3 die natürliche Abbildung $\pi_1(M \setminus N) \to \pi_1(M)$ ein Isomorphismus ist. In unserer Situation ist die reelle Kodimension zumindest 4, allerdings ist T nicht unbedingt eine glatte Untervarietät. Man kann aber mit einer Stratifizierung von T durch glatte Untervarietäten arbeiten und so das Ergebnis erhalten.

vor. Die Surjektivität folgt aus Aufgabe 28.3. (3). Der Monoidhomomorphismus

$$M \hookrightarrow \Gamma \xrightarrow{\gamma} \mathbb{Z}$$

führt zu einem $\mathbb{C}$-Algebrahomomorphisums

$$\mathbb{C}[M] \longrightarrow \mathbb{C}[\mathbb{Z}] \cong \mathbb{C}[W, W^{-1}]$$

und damit zu einem Morphismus der zugehörigen Spektren, der $\mathbb{C}$-Spektren, und der entsprechenden metrischen Räume, also zu einer (in der natürlichen Topologie) stetigen Abbildung

$$\gamma^*\colon\ \mathbb{C}^\times \longrightarrow Y = \operatorname{Spek}\left(\mathbb{C}[M]\right)_{\mathbb{C}}.$$

Da diese Abbildung über $\operatorname{Spek}\left(\mathbb{C}[\Gamma]\right)_{\mathbb{C}} \cong (\mathbb{C}^\times)^r$ faktorisiert, liegt das Bild dieser Abbildung ganz in $Y \setminus q(T)$. Die Einschränkung auf den Einheitskreis $S^1 \subseteq \mathbb{C}^\times$ ist natürlich ebenfalls stetig. (4). Wir haben ein kommutatives Diagramm

$$\begin{array}{ccccc} M & \longrightarrow & \Gamma & \xrightarrow{\gamma} & \mathbb{Z} \\ \downarrow & & \downarrow & & \downarrow \cdot m \\ \mathbb{N}^r & \longrightarrow & \mathbb{Z}^r & \xrightarrow{\tilde{\gamma}} & \mathbb{Z}\,, \end{array}$$

wobei $\tilde{\gamma}$ durch $\tilde{\gamma}(e_j) := \gamma(me_j)$ definiert ist. Diesem Diagramm entspricht das Diagramm

$$\begin{array}{ccc} \mathbb{C}^\times & \xrightarrow{\tilde{\gamma}^*} & \mathbb{C}^r \\ t^m \downarrow & & \downarrow \\ \mathbb{C}^\times & \xrightarrow{\gamma^*} & Y\ . \end{array}$$

Die Liftung spielt sich nun im Wesentlichen links ab, d.h. es muss der einfach geschlossene Weg

$$\iota\colon\ [0, 2\pi] \longrightarrow \mathbb{C}^\times,\ s \longmapsto e^{si},$$

bezüglich der m-ten Potenz $t \mapsto t^m$ geliftet werden. Dies geschieht aber durch die Zuordnung

$$\tilde{\iota}\colon\ [0, 2\pi] \longrightarrow \mathbb{C}^\times,\ s \longmapsto e^{\frac{si}{m}}.$$

Die j-te Komponente des Endpunkts dieser Liftung in $\mathbb{C}^r$ ist

$$\tilde{\gamma}_j^*\tilde{\iota}(2\pi) \ = \ \tilde{\gamma}_j^*\left(e^{\frac{2\pi i}{m}}\right) \ = \ \left(e^{\frac{2\pi i}{m}}\right)^{\tilde{\gamma}(e_j)} \ = \ \left(e^{\frac{2\pi i}{m}}\right)^{\gamma(me_j)} \ = \ e^{\frac{2\pi i\gamma(me_j)}{m}}.$$

Durch diese Zahlen ist auch der zu γ gehörende Charakter $F(\gamma)$ aus Teil (2) gegeben. □

Bemerkung 28.2. Wir betrachten eine Graduierung des Polynomringes $\mathbb{C}[X_1, \ldots, X_r]$ durch einen surjektiven Gruppenhomomorphismus

$$\delta\colon\ \mathbb{Z}^r \longrightarrow \mathbb{Z}/(\ell) := D$$

in eine endliche zyklische Gruppe. Es sei vorausgesetzt, dass $\delta(e_j)$ ein Erzeuger von $\mathbb{Z}/(\ell)$ für jeden Standardvektor $e_j \in \mathbb{Z}^r$ ist. Dann ist die zugehörige

Operation der Charaktergruppe $G = D^\vee = \mu_\ell(\mathbb{C})$ auf $\mathbb{C}^r \setminus \{0\}$ fixpunktfrei. Zu $x \neq 0$ sei $x_j \neq 0$. Für jeden Charakter $\chi \neq 1$ gilt

$$\chi(x) = (\ldots, \chi(\delta(e_j))x_j, \ldots) \neq (\ldots, x_j, \ldots),$$

da $\delta(e_j)$ nach Voraussetzung ein Erzeuger ist und somit $\chi(\delta(e_j)) \neq 1$ ist. Bei $r \geq 2$ ist in einem solchen Fall die Fundamentalgruppe von

$$\operatorname{Spek}\left(\mathbb{C}[X_1, \ldots, X_r]^G\right)_{\mathbb{C}} \setminus \{P\}$$

(wobei P das Bild des Nullpunktes sei) aufgrund von Satz 28.1 gleich $\mathbb{Z}/(\ell)$.

Beispiel 28.3. Wir betrachten die durch

$$\delta\colon\ \mathbb{Z}^2 \longrightarrow \mathbb{Z}/(\ell) =: D$$

mit

$$\delta(e_1) = 1,\ \delta(e_2) = \ell - 1$$

gegebene Graduierung auf $\mathbb{C}[U, V]$, die der linearen Operation der Matrizen

$$\begin{pmatrix} \zeta^i & 0 \\ 0 & \zeta^{-i} \end{pmatrix},\ i = 1, \ldots, \ell - 1$$

zu einer ℓ-ten primitiven Einheitswurzel ζ entspricht, vergleiche dazu auch Beispiel 3.16 und Beispiel 7.13. Der Kern ist durch

$$\Gamma = \langle \ell e_1, e_1 + e_2 \rangle$$

und das Monoid durch

$$M = \langle \ell e_1, \ell e_2, e_1 + e_2 \rangle$$

gegeben, der Invariantenring ist $\mathbb{C}[X, Y, Z](XY - Z^\ell)$. Die Bedingungen von Bemerkung 28.2 sind dabei erfüllt, es ist also $0 \in \mathbb{C}^2$ der einzige Fixpunkt und die Operation auf $\mathbb{C}^2 \setminus \{0\}$ ist fixpunktfrei. Daher kann man Satz 28.1 anwenden und erhält, dass die Fundamentalgruppe des punktierten Spektrum des Invariantenringes, also

$$\operatorname{Spek}\left(\mathbb{C}[X, Y, Z]/(XY - Z^\ell)\right)_{\mathbb{C}} \setminus \{P\},$$

gleich $\mathbb{Z}/(\ell)$ ist. Ein erzeugendes Element der Fundamentalgruppe wird auf der Monoidebene (bzw. auf dem Differenzengitter) durch

$$\gamma\colon\ \Gamma = \operatorname{kern}\delta \longrightarrow \mathbb{Z}$$

mit

$$\gamma(\ell e_1) = 1,\ \gamma(e_1 + e_2) = 0 \text{ und } \gamma(\ell e_2) = -1$$

gegeben. Dieser Homomorphismus lässt sich nicht nach $\mathbb{Z}^2$ fortsetzen, allerdings lässt sich das ℓ-fache davon fortsetzen. Auf der Ringebene entspricht dies dem $\mathbb{C}$-Algebrahomomorphismus

$$\varphi\colon\ \mathbb{C}[X, Y, Z]/(XY - Z^\ell) \longrightarrow \mathbb{C}[W, W^{-1}]$$

mit $\varphi(X) = W$, $\varphi(Y) = W^{-1}$ und $\varphi(Z) = 1$, was wiederum der stetigen Abbildung

$$\mathbb{C}^\times \longrightarrow \operatorname{Spek}\left(\mathbb{C}[X, Y, Z]/(XY - Z^\ell)\right)_{\mathbb{C}},\ t \longmapsto (t, t^{-1}, 1),$$

(bzw. ins punktierte Spektrum) entspricht. Somit ist

$$[0,2\pi] \longrightarrow \operatorname{Spek}\left(\mathbb{C}[X,Y,Z]/(XY-Z^\ell)\right)_{\mathbb{C}} \setminus \{P\},\ s \longmapsto \left(e^{is},\, e^{-is},\, 1\right),$$

ein Erzeuger der lokalen Fundamentalgruppe dieses Monoidringes.

Beispiel 28.4. Wir betrachten die durch

$$\delta\colon\ \mathbb{Z}^r \longrightarrow \mathbb{Z}/(\ell) =: D$$

mit

$$\delta(e_j) = 1 \text{ für alle } j$$

gegebene Graduierung auf $\mathbb{C}[X_1,\ldots,X_r]$, die der linearen Operation der Matrizen

$$\begin{pmatrix} \zeta^i & 0 & \cdots & \cdots & 0 \\ 0 & \zeta^i & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & \zeta^i & 0 \\ 0 & \cdots & \cdots & 0 & \zeta^i \end{pmatrix},\ i = 1,\ldots,\ell-1\,,$$

zu einer ℓ-ten primitiven Einheitswurzel ζ entspricht. Nach Lemma 9.7 ist der Invariantenring zu dieser Operation der ℓ-te Veronese-Ring

$$\mathbb{C}[X_1,\ldots,X_r]^{(\ell)}\,.$$

Die Bedingungen von Bemerkung 28.2 sind dabei erfüllt, es ist also $0 \in \mathbb{C}^r$ der einzige Fixpunkt und die Operation auf $\mathbb{C}^r \setminus \{0\}$ ist fixpunktfrei. Daher kann man bei $r \geq 2$ Satz 28.1 anwenden und erhält, dass die Fundamentalgruppe des punktierten Spektrum des Invariantenringes, also

$$\operatorname{Spek}\left(\mathbb{C}[X_1,\ldots,X_r]^{(\ell)}\right)_{\mathbb{C}} \setminus \{P\}\,,$$

gleich $\mathbb{Z}/(\ell)$ ist. Ein erzeugendes Element der Fundamentalgruppe wird auf der Monoidebene (bzw. auf dem Differenzengitter) durch den Homomorphismus

$$\gamma\colon\ \Gamma = \operatorname{kern}\delta \longrightarrow \mathbb{Z}$$

gegeben, der die Erzeuger e_j des umgebenden $\mathbb{Z}^r$ auf $\frac{1}{\ell}$ abbildet. Somit wird jeder Erzeuger des Monoids auf 1 abgebildet. Auf der Ringebene entspricht dies dem $\mathbb{C}$-Algebrahomomorphismus

$$\varphi\colon\ \mathbb{C}[X_1,\ldots,X_r]^{(\ell)} \longrightarrow \mathbb{C}[W,W^{-1}]$$

mit

$$\varphi(X^\nu) \,=\, W^{\frac{|\nu|}{\ell}}$$

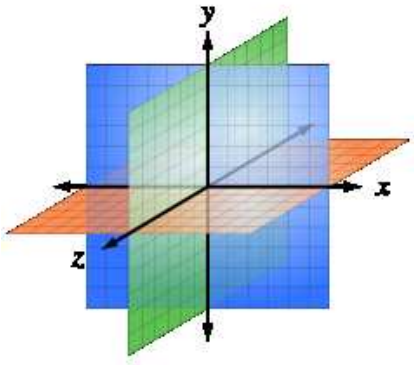
für alle Monome X^ν aus dem Veronese-Ring (die Erzeuger des Veronese-Ringes, also die Monome X^ν, $|\nu| = \ell$, werden einfach auf W abgebildet). Dies führt wiederum zur stetigen Abbildung

$$\mathbb{C}^\times \longrightarrow \operatorname{Spek}\left(\mathbb{C}[X_1,\ldots,X_r]^{(\ell)}\right)_{\mathbb{C}},\ t \longmapsto (t:\ |\nu| = \ell)$$

(bzw. ins punktierte Spektrum). Somit ist

$$[0,2\pi] \longrightarrow \operatorname{Spek}\left(\mathbb{C}[X_1,\ldots,X_r]^{(\ell)}\right)_{\mathbb{C}} \setminus \{P\},\ s \longmapsto \left(e^{is}:\ |\nu| = \ell\right),$$

ein Erzeuger der lokalen Fundamentalgruppe des Veronese-Ringes.



Außerhalb der drei schwarzen Achsen, die Kodimension 2 besitzen, ist die Operation fixpunktfrei. Die relevanten Wege verlaufen ganz im Komplement der drei Ebenen. Das reelle Bild lässt nicht erkennen, dass dieses Komplement im komplexen (auch einfach) zusammenhängend ist.

Beispiel 28.5. Wir betrachten die durch

$$\delta\colon\ \mathbb{Z}^3 \longrightarrow \mathbb{Z}/(2) \times \mathbb{Z}/(2) =: D$$

mit

$$\delta(e_1) = (1,0),\ \delta(e_2) = (0,1),\ \delta(e_3) = (1,1)$$

festgelegte Graduierung auf $\mathbb{C}[U,V,W]$. Die zugehörige lineare Operation auf dem $\mathbb{C}^3$ ist durch die Matrizen

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

gegeben. Die drei letzten Matrizen besitzen jeweils eine Fixgerade, daher ist die Operation auf $\mathbb{C}^3 \setminus \{0\}$ nicht fixpunktfrei, dagegen ist die Operation auf $X = \mathbb{C}^3 \setminus Z$, wobei $Z = \mathbb{C}e_1 \cup \mathbb{C}e_2 \cup \mathbb{C}e_3$ die Vereinigung der Achsen bezeichnet, frei. Da Z die (komplexe) Kodimension 2 besitzt, ist X einfach zusammenhängend. Der Invariantenring ist $\mathbb{C}[U^2,V^2,W^2,UVW]$ mit der Relation $(UVW)^2 = U^2V^2W^2$. Daher ist nach Satz 28.1 die Fundamentalgruppe von $\operatorname{Spek}\left(\mathbb{C}[U^2,V^2,W^2,UVW]\right)_{\mathbb{C}} \setminus q(Z)$ gleich $\mathbb{Z}/(2) \times \mathbb{Z}/(2)$.

Beispiel 28.6. Zum Restklassenhomomorphismus

$$\delta\colon\ \mathbb{Z} \longrightarrow \mathbb{Z}/(\ell) =: D$$

ist der Kern durch $\Gamma = \mathbb{Z}\ell$ gegeben. Die zugehörige Operation ist die von $\mu_\ell(\mathbb{C})$ auf $\mathbb{C}$ durch Multiplikation mit dem einzigen Fixpunkt 0 bzw. fixpunktfrei auf $\mathbb{C}^\times$. Die Quotientenabbildung ist durch das ℓ-te Potenzieren

$$\mathbb{C} \longrightarrow \mathbb{C},\ z \longmapsto z^\ell,$$

gegeben. Die Fundamentalgruppe von $\mathbb{C}^\times$ ist bekanntlich $\mathbb{Z}$. Hier kann man Satz 28.1 nicht anwenden, da der Raum, auf dem fixpunktfrei operiert wird, nämlich $\mathbb{C}^\times = \mathbb{C} \setminus \{0\}$, nicht einfach zusammenhängend ist.

Beispiel 28.7. Wir betrachten die durch

$$\delta\colon\ \mathbb{Z}^2 \longrightarrow \mathbb{Z}/(2) \times \mathbb{Z}/(2) =: D$$

mit

$$\delta(e_1) = (1,0),\ \delta(e_2) = (0,1)$$

festgelegte Graduierung auf $\mathbb{C}[U,V]$. Die zugehörige lineare Operation auf dem $\mathbb{C}^2$ ist durch die Matrizen

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

gegeben. Die zwei mittleren Matrizen besitzen jeweils eine Fixgerade, daher ist die Operation auf $\mathbb{C}^2 \setminus \{0\}$ nicht frei. Die Operation auf $X = \mathbb{C}^2 \setminus Z$, wobei $Z = \mathbb{C}e_1 \cup \mathbb{C}e_2$ das Achsenkreuz bezeichnet, ist frei, doch besitzt Z die Kodimension 1 in der Ebene. Der Invariantenring ist $\mathbb{C}[U^2, V^2]$, ein Polynomring in zwei Variablen, Satz 28.1 ist in diesem Fall nicht anwendbar.

28. Arbeitsblatt

Aufwärmaufgaben

Aufgabe 28.1. Es sei $a \in \mathbb{Z}$, $a \neq 0$. Wir betrachten die kurze exakte Sequenz

$$0 \longrightarrow \mathbb{Z} \xrightarrow{a} \mathbb{Z} \longrightarrow \mathbb{Z}/(a) \longrightarrow 0\,.$$

Zeige, dass dies zu einer kurzen exakten Sequenz

$$0 \cong \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/(a), \mathbb{Z}) \longrightarrow \mathbb{Z} \cong \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}) \longrightarrow \mathbb{Z} \cong \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}) \longrightarrow E \cong \mathbb{Z}/(a) \longrightarrow 0$$

führt.

Aufgabe 28.2. Es sei

$$\varphi\colon\ \mathbb{Z}^n \longrightarrow \mathbb{Z}^m$$

ein injektiver Gruppenhomomorphismus und

$$0 \longrightarrow \mathbb{Z}^n \xrightarrow{\varphi} \mathbb{Z}^m \longrightarrow D \longrightarrow 0$$

die zugehörige kurze exakte Sequenz. Zeige, dass dies zu einer exakten Sequenz

$$0 \longrightarrow \operatorname{Hom}_{\mathbb{Z}}(D, \mathbb{Z}) \longrightarrow \mathbb{Z}^m \cong \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}^m, \mathbb{Z}) \longrightarrow \mathbb{Z}^n \cong \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}^n, \mathbb{Z})$$

führt, wobei die Abbildung rechts nicht surjektiv sein muss.

Die nächste Aufgabe beruht auf dem Elementarteilersatz.

Aufgabe 28.3. Es sei

$$\varphi\colon\ \mathbb{Z}^n \longrightarrow \mathbb{Z}^n$$

ein injektiver Gruppenhomomorphismus und

$$0 \longrightarrow \mathbb{Z}^n \xrightarrow{\varphi} \mathbb{Z}^n \longrightarrow D \longrightarrow 0$$

die zugehörige kurze exakte Sequenz, wobei D endlich ist. Zeige, dass dies zu einer kurzen exakten Sequenz

$$0 \cong \operatorname{Hom}_{\mathbb{Z}}(D,\mathbb{Z}) \longrightarrow \mathbb{Z}^n \cong \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}^n,\mathbb{Z}) \longrightarrow \mathbb{Z}^n \cong \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}^n,\mathbb{Z}) \longrightarrow E \longrightarrow 0$$

führt, wobei E isomorph zu D ist.

Es sei R ein kommutativer Ring und M ein R-Modul. Der R-Modul

$$M^* = \operatorname{Hom}(M,R)$$

heißt der *duale Modul* zu M.

Aufgabe 28.4. Es sei R ein kommutativer Ring und sei

$$0 \longrightarrow L \longrightarrow M \longrightarrow N \longrightarrow 0$$

eine kurze exakte Sequenz von R-Moduln L, M, N. Zeige, dass dies zu einer exakten Sequenz

$$0 \longrightarrow N^* \longrightarrow M^* \longrightarrow L^*$$

der dualen Moduln führt.

Ein R-Modul M über einem Integritätsbereich heißt *Torsionsmodul*, wenn es zu jedem $v \in M$ ein $r \in R$, $r \neq 0$, mit $rv = 0$ gibt.

Aufgabe 28.5. Sei R ein Integritätsbereich und sei M ein R-Torsionsmodul. Zeige, dass der duale Modul $M^* = 0$ ist.

Aufgabe 28.6. Es sei M ein endlich erzeugtes Monoid und

$$\gamma\colon\ M \longrightarrow \mathbb{Z}$$

ein Monoidhomomorphismus mit der zugehörigen Spektrumsabbildung

$$\mathbb{C}^\times \cong \left(\operatorname{Spek}\left(\mathbb{C}[T,T^{-1}]\right)\right)_{\mathbb{C}} \longrightarrow \left(\operatorname{Spek}\left(\mathbb{C}[M]\right)\right)_{\mathbb{C}}$$

und dem induzierten stetigen geschlossenen Weg

$$S^1 \longrightarrow \left(\operatorname{Spek}\left(\mathbb{C}[M]\right)\right)_{\mathbb{C}}.$$

Zeige, dass dieser Weg nullhomotop ist, wenn der Monoidhomomorphismus γ durch $\mathbb{N}$ faktorisiert.

Aufgabe 28.7. Es sei M das punktierte Spektrum zu $R = \mathbb{C}[U,V,Z]/(U^2+V^2-Z^2)$. Man gebe einen expliziten Erzeuger der Fundamentalgruppe von M an.

Aufgabe 28.8. Es sei

$$A = \begin{pmatrix} \xi_1 & 0 & \cdots & 0 \\ 0 & \xi_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \xi_n \end{pmatrix}$$

eine Diagonalmatrix, deren Einträge allesamt Einheitswurzeln ξ_j in einem Körper K seien. Zeige, dass die zugehörige lineare Operation der von A erzeugten zyklischen Gruppe auf dem $K^n \setminus \{0\}$ genau dann fixpunktfrei ist, wenn die Ordnungen der ξ_j übereinstimmen.

Aufgabe 28.9. Wir betrachten die lineare Operation der zyklischen Gruppe $\mathbb{Z}/(5)$ auf $\mathbb{C}^3$ durch Potenzen der Matrix

$$\begin{pmatrix} \xi & 0 & 0 \\ 0 & \xi & 0 \\ 0 & 0 & \xi^3 \end{pmatrix},$$

wobei ξ eine fünfte primitive Einheitswurzel sei. Bestimme den Invariantenring zu dieser Operation. Man gebe einen expliziten Erzeuger der lokalen Fundamentalgruppe des Spektrums dieses Invariantenringes an.

Aufgabe 28.10. Wir betrachten die lineare Operation der symmetrischen Gruppe S_2 auf dem $\mathbb{C}^2$ und es sei

$$\mathbb{C}^2 \setminus T \longrightarrow \left(\mathbb{C}^2 \backslash S_2\right) \setminus q(T)$$

die zugehörige Quotientenabbildung, wobei T der Fixraum der Operation sei. Beschreibe die induzierte Abbildung der Fundamentalgruppen.

Aufgabe 28.11. Es sei $G \subseteq \mathrm{GL}_n(K)$ eine nichttriviale Reflektionsgruppe. Zeige, dass zu einer fixpunktfreien, offenen G-invarianten Teilmenge $U \subseteq K^n$ das Komplement $K^n \setminus U$ eine Dimension $\geq n-1$ besitzt.

Eine endliche Untergruppe $G \subseteq \mathrm{GL}_n(K)$ über einem Körper K heißt *klein*, wenn sie keine Pseudoreflektion enthält.

Aufgabe 28.12. Es sei $G \subseteq \mathrm{GL}_n(\mathbb{C})$ eine kleine Gruppe. Zeige, dass es eine offene Menge $U \subseteq \left(\mathrm{Spek}\left(K[X_1,\ldots,X_n]^G\right)\right)_{\mathbb{C}}$ gibt, deren Fundamentalgruppe gleich G ist.

Aufgaben zum Abgeben

Aufgabe 28.13. (6 Punkte)

Wir betrachten die lineare Operation der zyklischen Gruppe $\mathbb{Z}/(3)$ auf $\mathbb{C}^4$ durch Potenzen der Matrix

$$\begin{pmatrix} \xi & 0 & 0 & 0 \\ 0 & \xi & 0 & 0 \\ 0 & 0 & \xi^2 & 0 \\ 0 & 0 & 0 & \xi^2 \end{pmatrix},$$

wobei ξ eine dritte primitive Einheitswurzel sei. Bestimme den Invariantenring zu dieser Operation. Man gebe einen expliziten Erzeuger der lokalen Fundamentalgruppe des Spektrums dieses Invariantenringes an.

Aufgabe 28.14. (4 Punkte)

Zeige, dass der singuläre Ort der affinen Varietät

$$V(A^2 - BCD) \subseteq \mathbb{A}^4_K$$

(über einem algebraisch abgeschlossenen Körper K) aus drei Geraden besteht, und dass diese die Bilder der Koordinatenachsen des $\mathbb{A}^3_K$ unter der in Beispiel 28.5 besprochenen Quotientenabbildung sind.

29. Vorlesung - Lineare Gruppen

Lineare Gruppen und Operationen

Wir besprechen einige Beispiele von typischen Operationen von unendlichen algebraischen Gruppen wie der allgemeinen linearen Gruppe oder der speziellen linearen Gruppe. Ein solches Beispiel - die Operation auf der Menge der Dreiecke - haben wir schon in Beispiel 1.1 und in der fünften Vorlesung besprochen.

Beispiel 29.1. Es sei K ein Körper und V ein endlichdimensionaler K-Vektorraum. Die natürliche Operation der allgemeinen linearen Gruppe $G = \mathrm{GL}(V)$ besitzt nur zwei Bahnen, nämlich den Nullpunkt 0 und $V \setminus \{0\}$. Je zwei von 0 verschiedene Vektoren können ja mit einem geeigneten $g \in G$ ineinander überführt werden. Hier sind also keine interessanten Invarianten zu erwarten.

Ein $g \in G$ transformiert aber nicht nur einen einzigen Punkt $v \in V$ (einen Vektor), sondern beliebige Teilmengen $T \subseteq V$. Die Frage, ob zwei Teilmengen $T_1, T_2 \subseteq V$ mittels einem $g \in G$ ineinander überführt werden können,

wird schnell kompliziert (die Menge der betrachteten Objekte muss im Allgemeinen kein Vektorraum mehr sein). Hier betrachten wir endliche geordnete Punktmengen. Wir fixieren eine Zahl $n \in \mathbb{N}$ und betrachten Punkttupel

$$(P_1, \ldots, P_n) \in V^n \, ,$$

die wir uns als eine geordnete Punktkonfiguration in V vorstellen. Die Punkte sind also durchnummeriert, und es ist auch der Fall erlaubt, dass $P_i = P_j$ ist. Die Operation der allgemeinen linearen Gruppe dehnt sich sofort auf diese Situation aus, und zwar ist die Operation durch

$$\mathrm{GL}\,(V) \times V^n \longrightarrow V^n, \, (g, v_1, v_2, \ldots, v_n) \longmapsto (g(v_1), g(v_2), \ldots, g(v_n)),$$

gegeben.

Im einfachsten Fall, bei $V = K$, geht es um die Operation der Einheitengruppe $K^\times$ auf K^n durch skalare komponentenweise Multiplikation. Die Bahnen sind neben dem Nullpunkt die punktierten Geraden durch den Nullpunkt. Außer den konstanten Funktionen gibt es keine invarianten Polynome. Die auf $K^n \setminus \{0\}$ eingeschränkte Operation besitzt den $n-1$-dimensionalen projektiven Raum als Quotienten.

Beispiel 29.2. Es sei K ein Körper und V ein n-dimensionaler K-Vektorraum. Es sei $r \in \mathbb{N}$ (man denke an $r \leq n$) und wir betrachten die Wirkungsweise von $\mathrm{GL}_r(K)$ auf dem r-fachen Produkt von V mit sich selbst, bei der ein r-Tupel $v_1, \ldots, v_r$ von r Vektoren aus V auf ein anderes, durch die Matrix $g \in \mathrm{GL}_r(K)$ bestimmtes r-Tupel abgebildet wird. Mit $g = \begin{pmatrix} a_{11} & \ldots & a_{1r} \\ \vdots & \ddots & \vdots \\ a_{r1} & \ldots & a_{rr} \end{pmatrix}$ interessieren wir uns also für die Abbildung

$$\begin{aligned} \mathrm{GL}_r(K) \times V^r \longrightarrow V^r(\begin{pmatrix} a_{11} & \ldots & a_{1r} \\ \vdots & \ddots & \vdots \\ a_{r1} & \ldots & a_{rr} \end{pmatrix}, v_1, v_2, \ldots, v_r) \\ \longmapsto \left(\sum_{i=1}^r a_{1i} v_i, \, \sum_{i=1}^r a_{2i} v_i, \, \ldots, \, \sum_{i=1}^r a_{ri} v_i \right). \end{aligned}$$

Ein Tupel wird also stets auf ein Tupel aus Linearkombinationen der Einträge abgebildet. Daher ist der von $v_1, \ldots, v_r$ erzeugte K-Untervektorraum gleich dem vom Bildtupel $g(v_1, \ldots, v_r)$ erzeugten Untervektorraum. Wenn die $v_1, \ldots, v_r$ linear unabhängig sind, so gilt dies auch für das Bildtupel. Für einen r-dimensionalen Untervektorraum $U \subseteq V$ und zwei Basen von U gibt es stets einen Automorphismus von U, der die eine Basis in die andere Basis überführt. Wenn man also die Operation von $\mathrm{GL}_r(K)$ auf die (offene und dichte) Teilmenge $T \subseteq V^r$ einschränkt, die aus allen linear unabhängigen r-Tupeln besteht, so entsprechen die Bahnen der Operation den r-dimensionalen Untervektorräumen von V, und die Elemente der einzelnen

Bahnen durchlaufen sämtliche Basen des zugehörigen Raumes. Die Bahnen der Operation auf ganz V^r sind schwieriger zu charakterisieren.

Wir beschreiben die algebraische Version dieser Operation. Die linearen Funktionen auf dem der Operation zugrunde liegenden Vektorraum $W = V^r$ sind die Linearformen $f = (f_1, \ldots, f_r)$ mit

$$f(v_1, \ldots, v_r) \;=\; f_1(v_1) + \ldots + f_r(v_r).$$

Dabei sind die f_i Linearformen auf V, die wir direkt als Linearformen auf V^r über die i-te Projektion auffassen. Zu $g \in \mathrm{GL}_r(K)$ und $f = (f_1, \ldots, f_r)$ ist die verknüpfte Abbildung gleich

$$\begin{aligned}
(fg)\,(v_1, \ldots, v_r) &= f\left(\sum_{i=1}^r a_{1i}v_i, \sum_{i=1}^r a_{2i}v_i, \ldots, \sum_{i=1}^r a_{ri}v_i\right) \\
&= f_1\left(\sum_{i=1}^r a_{1i}v_i\right) + f_2\left(\sum_{i=1}^r a_{2i}v_i\right) + \ldots + f_r\left(\sum_{i=1}^r a_{ri}v_i\right) \\
&= \sum_{i=1}^r a_{1i}f_1\,(v_i) + \sum_{i=1}^r a_{2i}f_2\,(v_i) + \ldots + \sum_{i=1}^r a_{ri}f_r\,(v_i) \\
&= \sum_{i,j} a_{ji}f_j\,(v_i) \\
&= \sum_{j=1}^r a_{j1}f_j\,(v_1) + \sum_{j=1}^r a_{j2}f_j\,(v_2) + \ldots + \sum_{j=1}^r a_{jr}f_j\,(v_r) \\
&= \left(\sum_{j=1}^r a_{j1}f_j, \sum_{j=1}^r a_{j2}f_j, \ldots, \sum_{j=1}^r a_{jr}f_j\right)(v_1, \ldots, v_r)\,.
\end{aligned}$$

Daher ist

$$\begin{aligned}
fg &= (f_1, \ldots, f_r)\,g \\
&= \left(\sum_{j=1}^r a_{j1}f_j, \sum_{j=1}^r a_{j2}f_j, \ldots, \sum_{j=1}^r a_{jr}f_j\right).
\end{aligned}$$

Es sei nun $V = K^n$, so dass wir die Gesamtsituation mit Variablen schreiben können. Zum Vektorraum V^r gehört der Polynomring

$$K[X_{ij}\,, 1 \le i \le n,\, 1 \le j \le r]\,.$$

Dabei repräsentieren die X_{ij}, $1 \le i \le n$, die Koordinatenfunktionen der j-ten Kopie des Vektorraums K^n. Die Variable X_{ij} ist die j-te Projektion von V^r auf $V = K^n$ gefolgt von der i-ten Projektion p_i von K^n auf K. Somit ist (es steht p_i an der j-ten Stelle)

$$\begin{aligned}
X_{ij}g &= (0, \ldots, p_i, 0, \ldots, 0)\,g \\
&= (a_{j1}p_i, \ldots, a_{jr}p_i) \\
&= \sum_{k=1}^r a_{jk}X_{ik}.
\end{aligned}$$

Wenn eine Linearform (also eine Linearkombination aller X_{ij}) in Matrixform als

$$\begin{pmatrix} c_{11} & c_{12} & \ldots & c_{1r} \\ c_{21} & c_{22} & \ldots & c_{2r} \\ \vdots & \vdots & \ddots & \vdots \\ c_{n1} & c_{n2} & \ldots & c_{nr} \end{pmatrix}$$

gegeben ist, wobei die c_{ij} die Koeffizienten zu X_{ij} bezeichnen, so erhält man die durch g transformierte Linearform, indem man die Matrix von rechts mit der transponierten Matrix zu g multipliziert, also

$$\begin{pmatrix} c'_{11} & c'_{12} & \ldots & c'_{1r} \\ c'_{21} & c'_{22} & \ldots & c'_{2r} \\ \vdots & \vdots & \ddots & \vdots \\ c'_{n1} & c'_{n2} & \ldots & c'_{nr} \end{pmatrix} = \begin{pmatrix} c_{11} & c_{12} & \ldots & c_{1r} \\ c_{21} & c_{22} & \ldots & c_{2r} \\ \vdots & \vdots & \ddots & \vdots \\ c_{n1} & c_{n2} & \ldots & c_{nr} \end{pmatrix} \circ \begin{pmatrix} a_{11} & \ldots & a_{1r} \\ \vdots & \ddots & \vdots \\ a_{r1} & \ldots & a_{rr} \end{pmatrix}^{tr} .$$

Damit liegt eine Operation der $\mathrm{GL}_r(K)$ auf dem Polynomring in nr Variablen vor. Um invariante Polynome zu bekommen, schränken wir die Operation auf die spezielle lineare Gruppe $\mathrm{SL}_r(K) \subseteq \mathrm{GL}_r(K)$ ein. Dann sind sämtliche r-Minoren der Variablenmatrix

$$\begin{pmatrix} X_{11} & X_{12} & \ldots & X_{1r} \\ X_{21} & X_{22} & \ldots & X_{2r} \\ \vdots & \vdots & \ddots & \vdots \\ X_{n1} & X_{n2} & \ldots & X_{nr} \end{pmatrix}$$

invariant unter der Gruppenoperation. Dazu betrachten wir die universelle alternierende Abbildung

$$V^r \longrightarrow \bigwedge^r V, \, (v_1, \ldots, v_r) \longmapsto v_1 \wedge \ldots \wedge v_r.$$

Diese Abbildung ist nach einer geeigneten Verallgemeinerung von Korollar 80.7 (Mathematik (Osnabrück 2009-2011)) invariant unter der Gruppenoperation (dafür braucht man, dass die Determinanten von g gleich 1 sind). Die r-Minoren sind Linearformen auf dem r-ten Dachprodukt.

Definition 29.3. Zu einem K-Vektorraum V und einer natürlichen Zahl r nennt man die Menge der r-dimensionalen Untervektorräume $U \subseteq V$ die r-te *Graßmann-Varietät*. Sie wird mit $G(r, V)$ und bei $V = K^n$ mit $G(r, n)$ bezeichnet.

Nach Beispiel 29.2 ist $G(r, V)$ der Bahnenraum zur dort beschriebenen Operation der $\mathrm{GL}_r(K)$ auf $T \subseteq V^r$, wobei T aus den linear unabhängigen r-Tupeln besteht. Dieses T ist in der Zariski-Topologie eine offene Teilmenge und bei $K = \mathbb{R}$ oder $\mathbb{C}$ auch in der metrischen Topologie offen. Man kann $G(r, V)$ mit der Quotiententopologie unter der Quotientenabbildung versehen. Im metrischen Fall erhält man sogar eine Mannigfaltigkeitsstruktur auf $G(r, V)$, man spricht dann von der Graßmann-Mannigfaltigkeit.

Beispiel 29.4. Sei K ein Körper. Wir betrachten Paare von Matrizen

$$(B, C)\,,$$

wobei B eine $m \times n$-Matrix und C eine $n \times k$-Matrix ist. Es gibt also insgesamt $n(k+m)$ Koordinaten. Die allgemeine lineare Gruppe $G = \mathrm{GL}_n(K)$ operiert auf der Menge dieser Matrizenpaare in folgender Weise: Zu $A \in \mathrm{GL}_n(K)$ setzen wir

$$A \cdot (B, C) \;:=\; (BA^{-1}, AC).$$

Dass eine Operation vorliegt, folgt aus

$$\begin{aligned} A_1 \cdot (A_2 \cdot (B, C)) &= A_1 \cdot \left(BA_2^{-1}, A_2C\right) \\ &= ((BA_2^{-1})A_1^{-1}, A_1(A_2C)) \\ &= (B(A_2^{-1})A_1^{-1}), (A_1A_2)C) \\ &= (B(A_1A_2)^{-1}, (A_1A_2)C) \\ &= (A_1A_2) \cdot (B, C), \end{aligned}$$

woraus auch die Wahl der Reihenfolge und der Grund der Invertierung klar wird. Mit Hilfe der Variablenmatrizen

$$X = \begin{pmatrix} X_{11} & X_{12} & \dots & X_{1n} \\ X_{21} & X_{22} & \dots & X_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ X_{m1} & X_{m2} & \dots & X_{mn} \end{pmatrix} \text{ und } Y = \begin{pmatrix} Y_{11} & Y_{12} & \dots & Y_{1k} \\ Y_{21} & Y_{22} & \dots & Y_{2k} \\ \vdots & \vdots & \ddots & \vdots \\ Y_{n1} & Y_{n2} & \dots & Y_{nk} \end{pmatrix}$$

kann man einfach invariante Polynome aus $R = K[X, Y]$ angeben, nämlich die Einträge der Produktmatrix XY, also die Ausdrücke der Form

$$F_{ij} \;:=\; X_{i1}Y_{1j} + X_{i2}Y_{2j} + \ldots + X_{in}Y_{nj}.$$

Die Invarianz dieser Formen folgt direkt aus der Invarianz der Produktabbildung

$$\psi\colon\ \mathrm{Mat}_{m\times n}(K) \times \mathrm{Mat}_{n\times k}(K) \longrightarrow \mathrm{Mat}_{m\times k}(K),\ (B, C) \longmapsto BC,$$

welche sich direkt aus

$$\psi(A \cdot (B, C)) \;=\; \psi(BA^{-1}, AC) \;=\; BA^{-1}AC \;=\; BC \;=\; \psi(B, C)$$

ergibt. Darüber hinaus kann man zeigen, dass der Invariantenring von den F_{ij} erzeugt wird und auch eine explizite Restklassendarstellung ist bekannt: Wenn man den Polynomring $K[W] = K[W_{ij},\ 1 \le i \le m,\ 1 \le j \le k]$ heranzieht und die surjektive Abbildung

$$\pi\colon\ K[W] \longrightarrow R^G,\ W_{ij} \longmapsto F_{ij},$$

betrachtet, so wird der Kern von π durch sämtliche $n+1$-Minoren der Variablenmatrix W erzeugt. Dieser Invariantenring ist daher ein sogenannter Minorenring (oder Determinantenring), und insbesondere lassen sich Minorenringe als Invariantenringe realisieren.

Wenn beispielsweise $n = 1$ ist, so gibt es die Variablen $X_1, \ldots, X_m$ und $Y_1, \ldots, Y_k$ und es ist

$$F_{ij} \;=\; X_iY_j.$$

Zwischen den F_{ij} bestehen die Relationen

$$F_{ij}F_{rs} = X_iY_jX_rY_s = X_iY_sX_rY_j = F_{is}F_{rj},$$

d.h.

$$F_{ij}F_{rs} - F_{is}F_{rj} = 0.$$

Diese Relationen sind die 2-Minoren der Matrix $(W_{ij})_{ij}$. In diesem Fall ist der Invariantenring sogar ein Monoidring.

Affin-algebraische Gruppen

Definition 29.5. Sei K ein Körper. Eine *affin-algebraische Gruppe* (über K) ist eine Gruppe G der Form

$$G = (\mathrm{Spek}\,(H))\,(K),$$

wobei H eine kommutative endlich erzeugte K-Hopf-Algebra ist.

Eine affin-algebraische Gruppe ist also die Menge der K-Punkte eines affinen Gruppenschemas von endlichem Typ. Dazu gehören die endlichen Gruppen, die additive Gruppe $(K, +, 0)$, die multiplikative Gruppe $(K^\times, \cdot, 1)$, die allgemeine lineare Gruppe, die spezielle lineare Gruppe.

Definition 29.6. Sei K ein algebraisch abgeschlossener Körper und $\mathrm{GL}_n(K)$ die Gruppe der invertierbaren $n \times n$-Matrizen. Eine Zariski-abgeschlossene Untergruppe $G \subseteq \mathrm{GL}_n(K)$ nennt man eine *lineare Gruppe* (oder eine *linear-algebraische Gruppe*).

Man kann zeigen, dass affin-algebraische Gruppen und lineare Gruppen äquivalente Konzepte sind. Das erste Konzept ist begrifflich stärker, während das zweite Konzept die typischen Beispiele abdeckt. Der Zusammenhang beruht im Wesentlichen auf der Hopf-Interpretation der allgemeinen linearen Gruppe, siehe Beispiel 18.6.

Wir reformulieren Definition 18.9 für eine affin-algebraische Gruppe.

Definition 29.7. Zu einer affin-algebraischen Gruppe G über einem Körper K, die durch die kommutative K-Hopf-Algebra H gegeben sei, nennt man eine Operation von G auf einer kommutativen K-Algebra R *algebraisch* (oder *regulär*), wenn sie durch eine Kooperation von H auf R gegeben ist.

29. Arbeitsblatt

Aufwärmaufgaben

Die folgende Aufgabe liefert eine Verallgemeinerung von Korollar 80.7 (Mathematik (Osnabrück 2009-2011)).

Aufgabe 29.1. Zeige folgende Aussage über das Dachprodukt: Es sei K ein Körper und V ein K-Vektorraum der Dimension n. Es seien $v_1, \ldots, v_r$ und $w_1, \ldots, w_r$ Vektoren in V, die miteinander in der Beziehung

$$\begin{pmatrix} w_1 \\ \vdots \\ w_r \end{pmatrix} = M \begin{pmatrix} v_1 \\ \vdots \\ v_r \end{pmatrix}$$

stehen, wobei M eine $r \times r$-Matrix bezeichnet. Dann gilt in $\bigwedge^r V$ die Beziehung

$$w_1 \wedge \ldots \wedge w_r = (\det M) v_1 \wedge \ldots \wedge v_r.$$

Aufgabe 29.2. Zeige, dass die multiplikative Gruppe $(\mathbb{C}^\times, 1, \cdot)$ eine lineare Gruppe ist.

Aufgabe 29.3. Zeige, dass die additive Gruppe $(\mathbb{C}, 0, +)$ eine lineare Gruppe ist.

Aufgabe 29.4. Zeige, dass $(\mathbb{Z}, +, 0)$ keine lineare Gruppe über $\mathbb{C}$ ist.

Aufgabe 29.5. Zeige, dass $(\mathbb{Z}, +, 0)$ keine affin-algebraische Gruppe über $\mathbb{C}$ ist.

Aufgabe 29.6. Zeige, dass $(\mathbb{Z}, +, 0)$, versehen mit der diskreten Topologie, über keinem Körper K eine affin-algebraische Gruppe ist.

Aufgabe 29.7. Bestimme den Zariski-Abschluss der von der Matrix $\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$ erzeugten Untergruppe $G \subseteq \mathrm{GL}_2(\mathbb{C})$.

Aufgabe 29.8. Zeige, dass das Produkt von zwei linearen Gruppen wieder eine lineare Gruppe ist.

Aufgabe 29.9. a) Sei K ein Körper. Zeige, dass die Einheitengruppe von K nicht zyklisch unendlich ist.

b) Sei R ein kommutativer Ring, dessen Charakteristik nicht zwei ist. Zeige, dass die Einheitengruppe von R nicht zyklisch unendlich ist.

c) Beschreibe einen kommutativen Ring, dessen Einheitengruppe zyklisch unendlich ist.

Wir erinnern an zwei Definitionen für Matrizen.

Eine $n \times n$-Matrix der Form

$$\begin{pmatrix} b_1 & * & \cdots & \cdots & * \\ 0 & b_2 & * & \cdots & * \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & b_{n-1} & * \\ 0 & \cdots & \cdots & 0 & b_n \end{pmatrix}$$

nennt man *obere Dreiecksmatrix*.

Eine $n \times n$-Matrix der Form

$$\begin{pmatrix} 1 & * & \cdots & \cdots & * \\ 0 & 1 & * & \cdots & * \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 1 & * \\ 0 & \cdots & \cdots & 0 & 1 \end{pmatrix}$$

nennt man (obere) *Scherungsmatrix*.

Aufgabe 29.10. Es sei K ein Körper. Zeige, dass die Menge der invertierbaren $n \times n$-oberen Dreiecksmatrizen über K eine Untergruppe der $\mathrm{GL}_n(K)$ ist.

Aufgabe 29.11. Es sei K ein Körper und $\mathrm{ODG}_n(K)$ die Gruppe der invertierbaren $n \times n$-oberen Dreiecksmatrizen über K. Zeige, dass es einen (natürlichen) surjektiven Gruppenhomomorphismus

$$\varphi\colon\ \mathrm{ODG}_n(K) \longrightarrow \left(K^\times, \cdot, 1\right)^n$$

gibt. Bestimme den Kern von φ.

Aufgabe 29.12. Es sei K ein Körper. Zeige, dass die Menge der invertierbaren $n \times n$-oberen Scherungsmatrizen über K eine Untergruppe der $\mathrm{SL}_n(K)$ ist.

Aufgabe 29.13. Es sei K ein Körper und $\mathrm{OSG}_n(K)$ die Gruppe der $n \times n$-oberen Scherungsmatrizen über K. Zeige, dass es einen (natürlichen) surjektiven Gruppenhomomorphismus

$$\varphi\colon\ \mathrm{OSG}_n(K) \longrightarrow (K, +, 0)^{n-1}$$

gibt. Bestimme den Kern von φ.

Zeige in den vorstehenden Aufgaben, dass jeweils eine lineare Gruppe (über einem nicht notwendigerweise algebraisch abgeschlossenen Körper) vorliegt, und dass die Gruppenhomomorphismen algebraisch definiert sind.

Aufgabe 29.14. Es sei K ein Körper und $\mathrm{OSG}_3(K)$ die Gruppe der 3×3-oberen Scherungsmatrizen über K. Zeige, dass es eine kurze exakte Sequenz

$$0 \longrightarrow K \longrightarrow \mathrm{OSG}_3(K) \longrightarrow K^2 \longrightarrow 0$$

gibt, und dass $\mathrm{OSG}_3(K)$ nicht isomorph zu K^3 ist.

Aufgaben zum Abgeben

Aufgabe 29.15. (4 Punkte)

Bestimme den Zariski-Abschluss der von der Matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ erzeugten Untergruppe $G \subseteq \mathrm{GL}_2(\mathbb{C})$.

Aufgabe 29.16. (4 Punkte)

Zeige, dass eine zyklische Untergruppe $G \subseteq \mathrm{GL}_n(\mathbb{C})$ bei $n \geq 2$ nicht Zariski-dicht ist.

Aufgabe 29.17. (8 Punkte)

Es sei K ein algebraisch abgeschlossener Körper. Zeige, dass $(\mathbb{Z}, +, 0)$ keine lineare Gruppe über K ist.

30. Vorlesung - Linear reduktive Gruppen I

Linear reduktive Gruppen

In den verbleibenden Vorlesungen möchten wir zeigen, dass die Invariantenringe zu algebraischen Operationen der allgemeinen linearen oder der speziellen linearen Gruppe über $\mathbb{C}$ endlich erzeugt sind. Der Schlüsselbegriff für diese Aussage ist die *lineare Reduktivität*, der eine Eigenschaft sämtlicher Darstellungen der Gruppe ist. Eine Darstellung einer Gruppe G ist einfach ein Gruppenhomomorphismus

$$G \longrightarrow \mathrm{GL}(V)$$

mit einem K-Vektorraum V. Wenn G eine affin-algebraische Gruppe über einem fixierten Körper K (der häufig als algebraisch abgeschlossen angenommen wird) ist, so interessiert man sich vor allem für Darstellungen in Vektorräume über diesem Körper. Ferner soll die Darstellung algebraisch sein. Diese Forderungen kommen in der folgenden Definition zum Ausdruck.

Definition 30.1. Es sei K ein Körper und sei G eine affin-algebraische Gruppe über K. Unter einer *K-rationalen Darstellung* von G versteht man einen Gruppenhomomorphismus

$$G \longrightarrow \mathrm{GL}\,(V)$$

mit einem endlichdimensionalen K-Vektorraum V (also eine Darstellung von G), die durch einen K-Hopf-Algebrahomomorphismus der Hopfalgebren zu G bzw. $\mathrm{GL}\,(V)$ induziert wird.

Dies ist äquivalent dazu, dass die Operation von G auf V, also die Abbildung

$$G \times V \longrightarrow V,$$

algebraisch ist, also durch eine Kooperation der Hopfalgebra H (zu G) auf dem Polynomring $K[V]$ gegeben ist. Man sagt dann auch, dass G auf V K-rational operiert.

Für die multiplikative Gruppe $K^\times$ ist beispielsweise die Zuordnung

$$K^\times = \mathrm{GL}_1(K) \longrightarrow \mathrm{GL}_n(K)\,,\, t \longmapsto \begin{pmatrix} t^{a_1} & 0 & 0 & 0 \\ 0 & t^{a_2} & 0 & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & t^{a_n} \end{pmatrix},$$

mit $a_j \in \mathbb{Z}$ eine K-rationale Darstellung, für die additive Gruppe K ist beispielsweise die Zuordnung

$$K \longrightarrow \mathrm{GL}_2(K)\,,\, t \longmapsto \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix},$$

eine solche.

Zur Formulierung der linearen Reduktivität brauchen wir noch einige weitere Begriffe aus der Darstellungstheorie.

Definition 30.2. Eine Darstellung

$$\rho\colon\ G \longrightarrow \mathrm{GL}\,(V)$$

einer Gruppe G in einem K-Vektorraum V heißt *irreduzibel*, wenn $V \neq 0$ ist und wenn die einzigen G-invarianten Untervektorräume 0 und V sind.

Definition 30.3. Eine Darstellung

$$\rho\colon\ G \longrightarrow \mathrm{GL}\,(V)$$

einer Gruppe G in einem K-Vektorraum V heißt *vollständig reduzibel*, wenn V die direkte Summe aus G-invarianten Untervektorräumen ist, die jeweils irreduzibel sind.

Zwei Darstellungen

$$\rho_1\colon\ G \longrightarrow \mathrm{GL}\,(V_1)$$

und

$$\rho_2\colon\ G \longrightarrow \mathrm{GL}\,(V_2)$$

heißen *äquivalent*, wenn es eine bijektive K-lineare Abbildung

$$\varphi\colon V_1 \longrightarrow V_2$$

mit $\rho_2 = \varphi \circ \rho_1$ gibt (wobei φ als Isomorphismus zwischen den allgemeinen linearen Gruppen aufgefasst wird).

Definition 30.4. Eine affin-algebraische Gruppe G über einem Körper K heißt *linear reduktiv*, wenn jede K-rationale Darstellung von G vollständig reduzibel ist.

Wir werden später sehen, dass die allgemeine lineare Gruppe über $\mathbb{C}$ linear reduktiv ist, was auf maßtheoretischen Methoden beruht. Zunächst wenden wir uns endlichen (nichtmodularen) Gruppen und kommutativen Gruppen zu, die ebenfalls linear reduktiv sind.

Lineare Reduktivität von endlichen Gruppen

Wir brauchen zunächst das folgende einfache Lemma.

Lemma 30.5. *Es sei K ein Körper und G eine Gruppe, die auf den beiden K-Vektorräumen V und W linear operiere. Es sei $\varphi\colon V \to W$ eine G-verträgliche lineare Abbildung. Dann ist sowohl* $\operatorname{kern}\varphi$ *als auch* $\operatorname{bild}\varphi$ *G-invariant.*

Beweis. Sei $v \in \operatorname{kern}\varphi$ und $g \in G$. Wegen der Verträglichkeit von φ mit den Gruppenoperationen ist

$$\varphi(gv) = g(\varphi(v)) = g(0) = 0,$$

also ist $gv \in \operatorname{kern}\varphi$ und der Kern ist invariant. Bei $w \in \operatorname{bild}\varphi$, sagen wir $w = \varphi(v)$, und $g \in G$ ist wiederum

$$\varphi(gv) = g(\varphi(v)) = g(w),$$

also $gv \in \operatorname{bild}\varphi$ und das Bild ist ebenfalls invariant. □

Die folgenden Aussagen heißen *Lemma von Maschke* bzw. *Satz von Maschke*.

Lemma 30.6. *Es sei K ein Körper und G eine endliche Gruppe, deren Ordnung kein Vielfaches der Charakteristik von K sei. Es sei*

$$\rho\colon G \longrightarrow \mathrm{GL}(V)$$

eine Darstellung in einen endlichdimensionalen K-Vektorraum V und $U \subseteq V$ ein G-invarianter Untervektorraum. Dann gibt es einen G-invarianten Untervektorraum $W \subseteq V$ mit $V = U \oplus W$.[11]

[11] Einen solchen Unterraum nennt man ein *G-invariantes Komplement* von U.

Beweis. Aufgrund des Basisergänzungssatzes kann man $V = U \oplus W'$ mit einem K-Untervektorraum W' schreiben, und man hat eine Projektion (längs W')

$$\pi \colon V \longrightarrow U$$

mit $\pi \circ \iota = \mathrm{id}_U$, wobei ι die Einbettung $U \subseteq W$ bezeichnet. Wir betrachten die lineare Abbildung (mit $n = \mathrm{ord}\,(G)$; dies ist eine Einheit in K)

$$\psi \colon V \longrightarrow V,\, v \longmapsto \frac{1}{n} \sum_{g \in G} g^{-1}(\pi(g(v))).$$

Für $u \in U$ ist (wegen $g(u) \in U$ und da π auf U die Identität ist)

$$\begin{aligned} \psi(u) &= \frac{1}{n} \sum_{g \in G} g^{-1}(\pi(g(u))) \\ &= \frac{1}{n} \sum_{g \in G} g^{-1}(g(u)) \\ &= \frac{1}{n} \sum_{g \in G} u \\ &= u \end{aligned}$$

und das Bild von ψ ist gleich U, d.h. ψ ist ebenfalls eine Projektion auf U. Allerdings ist diese Projektion zusätzlich G-verträglich. Für $h \in G$ ist nämlich

$$\begin{aligned} \psi(hv) &= \frac{1}{n} \sum_{g \in G} g^{-1}(\pi(g(hv))) \\ &= \frac{1}{n} \sum_{f \in G} (hf^{-1})(\pi(f(v))) \\ &= h \left(\frac{1}{n} \sum_{f \in G} f^{-1}(\pi(f(v))) \right) \\ &= h\left(\psi(v)\right). \end{aligned}$$

Wir setzen nun $W := \ker \psi$. Als Kern einer mit der Operation verträglichen linearen Abbildung ist W nach Lemma 30.5 ebenfalls G-invariant, und es ist offenbar $V = U \oplus W$. $\square$

Heinrich Maschke (1853-1908)

Satz 30.7. *Es sei K ein Körper und G eine endliche Gruppe, deren Ordnung kein Vielfaches der Charakteristik von K sei. Dann ist G linear reduktiv.*

Beweis. Es sei

$$\rho\colon\ G \longrightarrow \mathrm{GL}\,(V)$$

eine Darstellung von G. Wir müssen zeigen, dass die Darstellung vollständig reduzibel ist, also eine direkte Summe aus irreduziblen Darstellungen ist. Wir beweisen die Aussage durch Induktion über die Dimension von V. Bei $\dim(V) = 0, 1$ ist nichts zu zeigen. Wenn die Darstellung irreduzibel ist, so sind wir ebenfalls fertig. Andernfalls gibt es einen echten G-invarianten Untervektorraum $U \subset V$. Dieser hat nach Lemma 30.6 ein G-invariantes Komplement $W \subseteq V$. Nach Induktionsvoraussetzung besitzen U und W eine direkte Zerlegung in irreduzible Darstellungen. Dies überträgt sich auf V. □

Darstellungstheorie kommutativer Gruppen

Kommutative besitzen eine einfachere Darstellungstheorie, da nur eindimensionale Darstellungen irreduzibel sind. Dies ergibt sich aus dem sogenannten *Lemma von Schur* (der nächsten Aussage). Die Konsequenzen für die kommutativen affin-algebraischen Gruppen (beispielsweise die multiplikative und die additive Gruppe) sind aber unterschiedlich.

Lemma 30.8. *Es sei K ein Körper, G eine Gruppe und seien V_1, V_2 zwei K-Vektorräume mit zwei gegebenen irreduziblen Darstellungen $\rho_1\colon\ G \to \mathrm{GL}\,(V_1)$ und $\rho_2\colon\ G \to \mathrm{GL}\,(V_2)$. Es sei $\varphi\colon\ V_1 \to V_2$ eine lineare Abbildung mit*

$$\sigma_2 \circ \varphi \ = \ \varphi \circ \sigma_1$$

für alle $\sigma \in G$, wobei σ_i den zu σ gehörenden Automorphismus auf V_i bezeichnet. Dann ist $\varphi = 0$ oder aber φ definiert eine Äquivalenz der beiden Darstellungen.

Beweis. Es sei $\varphi \neq 0$. Wir müssen zeigen, dass φ ein Isomorphismus ist. Es sei $U := \operatorname{kern} \varphi$. Nach Lemma 30.5 ist U G-invariant. Wegen der Irreduzibilität von ρ_1 ist $U = 0$ oder $U = V_1$, wobei die zweite Möglichkeit wegen $\varphi \neq 0$ ausscheidet. Also ist der Kern trivial und damit ist nach Lemma 12.7 (Mathematik (Osnabrück 2009-2011)) φ injektiv. Es sei jetzt $W := \operatorname{bild} \varphi$. Nach Lemma 30.5 ist W ebenfalls G-invariant. Der Fall $W = 0$ ist wegen $\varphi \neq 0$ ausgeschlossen, also ist $W = V_2$ wegen der Irreduzibilität von ρ_2 und somit ist φ auch surjektiv. □

Issai Schur (1875-1941)

Korollar 30.9. *Es sei K ein algebraisch abgeschlossener Körper, G eine Gruppe und V ein endlichdimensionaler K-Vektorraum. Es sei $\rho\colon G \to \mathrm{GL}(V)$ eine irreduzible Darstellung und es sei $\varphi\colon V \to V$ eine lineare Abbildung mit*

$$\sigma \circ \varphi = \varphi \circ \sigma$$

für alle $\sigma \in G$. Dann ist φ eine Streckung.

Beweis. Wir können $\varphi \neq 0$ annehmen. Aufgrund der Voraussetzung an K besitzt φ einen Eigenwert λ. Wir betrachten $\varphi - \lambda \operatorname{Id}_V$. Da eine Streckung mit

jedem Endomorphismus vertauscht, gilt für $\varphi - \lambda \operatorname{Id}_V$ ebenfalls die Voraussetzung. Nach Lemma 30.8 ist also $\varphi - \lambda \operatorname{Id}_V$ ein Isomorphismus oder gleich 0. Da es einen nichttrivialen Kern (nämlich den Eigenraum zu λ) besitzt, muss $\varphi - \lambda \operatorname{Id}_V = 0$ sein, also ist φ ein skalares Vielfaches der Identität. □

Korollar 30.10. *Es sei K ein algebraisch abgeschlossener Körper und G eine kommutative Gruppe. Dann ist jede irreduzible Darstellung von G in einen endlichdimensionalen K-Vektorraum eindimensional.*

Beweis. Es sei

$$\rho\colon G \longrightarrow \mathrm{GL}(V)$$

eine irreduzible Darstellung. Wegen der Kommutativität von G gilt für die zu $\sigma, \tau \in G$ gehörenden linearen Abbildungen

$$\sigma \circ \tau = \tau \circ \sigma.$$

Aus Korollar 30.9, angewandt für festes τ und alle σ, folgt, dass τ eine Streckung ist. Dann sind aber überhaupt sämtliche Automorphismen der Darstellung Streckungen. Unter einer Streckung ist aber jeder Untervektorraum invariant, so dass in diesem Fall jeder Untervektorraum G-invariant ist. Dann muss aber wegen der Irreduzibilität V eindimensional sein. □

30. Arbeitsblatt

Aufwärmaufgaben

Aufgabe 30.1. Es sei K ein Körper und V ein K-Vektorraum, auf dem eine Gruppe G linear operiere. Es sei $W \subseteq V$ ein G-irreduzibler Untervektorraum und $U \subseteq V$ ein G-invarianter Untervektorraum. Zeige, dass $U \cap W$ gleich W oder gleich 0 ist.

Aufgabe 30.2. Zeige, dass zu jeder Darstellung einer Gruppe G in einen endlichdimensionalen K-Vektorraum V ein Charakter $G \to K^\times$ gehört.

Aufgabe 30.3. Es sei K ein Körper. Man gebe eine Darstellung von $\mathbb{Z}$ in einen endlichdimensionalen K-Vektorraum an, die nicht vollständig reduzibel ist.

Aufgabe 30.4. Es sei K ein Körper. Man gebe eine Darstellung von $(\mathbb{Q}^\times, \cdot, 1)$ in einen endlichdimensionalen K-Vektorraum an, die nicht vollständig reduzibel ist.

Aufgabe 30.5. Zeige, dass die additive Gruppe $(K,+,0)$ nicht linear reduktiv ist.

Wir erinnern an zwei Definitionen für Matrizen.

Eine $n \times n$-Matrix der Form

$$\begin{pmatrix} b_1 & * & \cdots & \cdots & * \\ 0 & b_2 & * & \cdots & * \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & b_{n-1} & * \\ 0 & \cdots & \cdots & 0 & b_n \end{pmatrix}$$

nennt man *obere Dreiecksmatrix*.

Eine $n \times n$-Matrix der Form

$$\begin{pmatrix} 1 & * & \cdots & \cdots & * \\ 0 & 1 & * & \cdots & * \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 1 & * \\ 0 & \cdots & \cdots & 0 & 1 \end{pmatrix}$$

nennt man (obere) *Scherungsmatrix*.

Aufgabe 30.6. Es sei K ein Körper. Zeige, dass die Menge der invertierbaren $n \times n$-oberen Dreiecksmatrizen über K eine Untergruppe der $\mathrm{GL}_n(K)$ ist.

Aufgabe 30.7. Es sei K ein Körper und $\mathrm{ODG}_n(K)$ die Gruppe der invertierbaren $n \times n$-oberen Dreiecksmatrizen über K. Zeige, dass es einen (natürlichen) surjektiven Gruppenhomomorphismus

$$\varphi\colon\ \mathrm{ODG}_n(K) \longrightarrow \left(K^\times, \cdot, 1\right)^n$$

gibt. Bestimme den Kern von φ.

Aufgabe 30.8. Es sei K ein Körper. Zeige, dass die Menge der invertierbaren $n \times n$-oberen Scherungsmatrizen über K eine Untergruppe der $\mathrm{SL}_n(K)$ ist.

Aufgabe 30.9. Es sei K ein Körper und $\mathrm{OSG}_n(K)$ die Gruppe der $n \times n$-oberen Scherungsmatrizen über K. Zeige, dass es einen (natürlichen) surjektiven Gruppenhomomorphismus

$$\varphi\colon\ \mathrm{OSG}_n(K) \longrightarrow (K,+,0)^{n-1}$$

gibt. Bestimme den Kern von φ.

Zeige in den vorstehenden Aufgaben, dass jeweils eine lineare Gruppe (über einem nicht notwendigerweise algebraisch abgeschlossenen Körper) vorliegt, und dass die Gruppenhomomorphismen algebraisch definiert sind.

Aufgabe 30.10. Es sei K ein Körper und $\mathrm{OSG}_3(K)$ die Gruppe der 3×3-oberen Scherungsmatrizen über K. Zeige, dass es eine kurze exakte Sequenz

$$0 \longrightarrow K \longrightarrow \mathrm{OSG}_3(K) \longrightarrow K^2 \longrightarrow 0$$

gibt, und dass $\mathrm{OSG}_3(K)$ nicht isomorph zu K^3 ist.

Aufgabe 30.11. Es sei K ein Körper und es sei $\psi \in \mathrm{GL}_n(K)$ eine Pseudoreflektion. Zeige, dass jede Konjugation von ψ ebenfalls eine Pseudoreflektion ist.

Aufgabe 30.12. Es sei K ein Körper, $G \subseteq \mathrm{GL}_n(K)$ eine Untergruppe und $H \subseteq G$ die von allen Pseudoreflektionen in G erzeugte Untergruppe. Zeige, dass H ein Normalteiler in G ist.

Aufgabe 30.13. Es sei K ein Körper, $G \subseteq \mathrm{GL}_n(K)$ eine endliche Untergruppe, deren Ordnung eine Einheit in K sei, und $H \subseteq G$ ein Normalteiler. Es sei $R = K[X_1, \ldots, X_n]^H$ der Invariantenring zu H, auf dem gemäß Proposition 5.1 (3) die Restklassengruppe G/H operiert. Zeige, dass es einen endlichdimensionalen Untervektorraum $W \subseteq R$ gibt, der R als K-Algebra erzeugt und auf dem die Operation von G/H linear ist.

Aufgabe 30.14. Wir betrachten die Gruppe

$$G = \{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}\} \subseteq \mathrm{GL}_2(K)$$

(K sei ein Körper der Charakteristik $\neq 2$) mit dem Normalteiler $S_2 \subseteq G$. Man gebe für den Invariantenring $K[U,V]^{S_2}$ zwei Algebraerzeugendensysteme aus jeweils zwei Erzeugern an, derart, dass G/S_2 auf dem einen System linear operiert und auf dem anderen nicht.

Aufgaben zum Abgeben

Aufgabe 30.15. (5 Punkte)

Es sei K ein Körper und $G \subseteq \mathrm{GL}_n(K)$ eine endliche Untergruppe, deren Ordnung eine Einheit in K sei. Zeige, dass der Invariantenring $R = K[X_1, \ldots, X_n]^G$ auch als Invariantenring zu einer kleinen Gruppe $G' \subseteq \mathrm{GL}_n(K)$ auftritt.

Aufgabe 30.16. (8 Punkte)

Es sei K ein algebraisch abgeschlossener Körper. Zeige, dass $(\mathbb{Z}, +, 0)$ keine lineare Gruppe über K ist.

31. Vorlesung - Linear reduktive Gruppen II

Invariantenringe bei linear reduktiver Gruppe

Wir möchten zeigen, dass der Invariantenring zu einer algebraischen Operation einer linear reduktiven Gruppe ein direkter Summand ist, woraus folgt, dass er endlich erzeugt ist. Wir beginnen mit äquivalenten Charakterisierungen von linear reduktiv.

Satz 31.1. *Es sei K ein algebraisch abgeschlossener Körper und G eine affin-algebraische Gruppe über K. Dann sind folgende Aussagen äquivalent.*

(1) *G ist linear reduktiv.*
(2) *Zu jeder K-rationalen Darstellung auf einem endlichdimensionalen K-Vektorraum V besitzt $V^G \subseteq V$ ein eindeutig bestimmtes G-Komplement $W \subseteq V$. Dabei gilt $(W^*)^G = 0$.*
(3) *Zu jeder K-rationalen Darstellung auf einem endlichdimensionalen K-Vektorraum V und jedem $v \in V^G$, $v \neq 0$, gibt es eine G-invariante Linearform $f \in V^*$ mit $f(v) \neq 0$.*
(4) *Zu jeder K-rationalen Darstellung auf einem endlichdimensionalen K-Vektorraum V und jedem G-Untervektorraum $U \subseteq V$ gibt es ein G-Komplement.*

Beweis. (1) $\Rightarrow$ (2). Es sei $V = V_1 \oplus \cdots \oplus V_r$ die Zerlegung in irreduzible Darstellungen. Wegen der Irreduzibilität ist $(V_i)^G = V_i \cap V^G$ gleich 0 oder gleich V_i, daher ist (nach Umordnung) $V^G = V_1 \oplus \cdots \oplus V_s$. Die direkte Summe der verbleibenden irreduziblen Unterräume, also $W = V_{s+1} \oplus \cdots \oplus V_r$ bilden ein G-invariantes Komplement. Wenn W' ein solches G-Komplement ist, so gilt wieder $W' \cap V_i = V_i$ oder $= 0$. Bei $W' \cap V_i = 0$ für ein $i \geq s+1$ würde die Dimension von W' zu klein werden, also muss $W' = W$ sein. Den Zusatz kann man für die an W beteiligten V_i getrennt beweisen. Es sei also

$$h\colon V_i \longrightarrow K$$

eine G-invariante Linearform. Bei $\dim(V_i) \geq 2$ und $h \neq 0$ wäre der Kern ein echter G-invarianter Untervektorraum im Widerspruch zur Irreduziblität von V_i. Bei $\dim(V_i) = 1$ und $h \neq 0$ wäre h eine Bijektion, und dann müsste G auf V_i identisch wirken. (2) $\Rightarrow$ (3). Wir betrachten die lineare Projektion

$$\pi\colon V \longrightarrow V^G$$

zur Zerlegung $V = V^G \oplus W$ mit dem G-invarianten Komplement W. Dabei ist $\pi(v) = v \neq 0$ und dazu gibt es eine Linearform $h\colon V^G \to K$ mit $h(v) \neq 0$. Die Linearform $h \circ \pi$ ist G-verträglich und leistet das Gewünschte. (3) $\Rightarrow$ (4).

Sei zunächst U irreduzibel. Die Räume $\mathrm{Hom}_K(U,V)$ und $\mathrm{Hom}_K(V,U)$ sind dual zueinander, und zwar über die Beziehung

$$\mathrm{Hom}_K(U,V) \times \mathrm{Hom}_K(V,U) \longrightarrow K,\ (\varphi,\psi) \longmapsto \mathrm{Spur}(\varphi \circ \psi).$$

Dabei ist $\varphi \circ \psi$ ein Endomorphismus auf V. Wir fassen die Inklusion $U \subseteq V$ als eine G-invariante lineare Abbildung, also als ein Element φ in $\mathrm{Hom}_K(U,V)^G$, auf. Nach (3), angewendet auf dieses Element, muss es ein G-invariantes $\psi \in \mathrm{Hom}_K(V,U) \cong \mathrm{Hom}_K(U,V)^*$ mit $\psi(\varphi) \neq 0$ geben, was $\mathrm{Spur}(\varphi \circ \psi) = \mathrm{Spur}(\psi \circ \varphi) \neq 0$ bedeutet. Die lineare Abbildung

$$\psi \circ \varphi \colon\ U \longrightarrow U$$

ist daher nicht die Nullabbildung, und sie ist G-invariant als Verknüpfung von zwei G-invarianten linearen Abbildungen. Nach Korollar 30.9 ist $\psi \circ \varphi$ eine Streckung, die wir zur Identität normieren können. Somit ist ψ eine G-invariante Projektion auf U und daher ist

$$V = U \oplus \mathrm{kern}\,\varphi.$$

Im allgemeinen Fall führen wir Induktion über die Dimension von V. Es sei

$$0 \neq U' \subseteq U$$

ein G-invarianter irreduzibler Untervektorraum. Nach der Vorüberlegung ist $V = U' \oplus V'$, wobei V' ebenfalls G-invariant ist. Es ist dann

$$U = U' \oplus (U \cap V').$$

Aufgrund der Induktionsvoraussetzung ist

$$V' = (U \cap V') \oplus W$$

mit einem G-invarianten Untervektorraum

$$W \subseteq V'$$

und daher ist

$$V = U' \oplus V' = U' \oplus (U \cap V') \oplus W = U \oplus W.$$

(4) $\Rightarrow$ (1). Induktion über die Dimension von V. □

Wir wollen zeigen, dass der Invariantenring zu einer algebraischen Operation einer linear reduktiven Gruppe auf einer K-Algebra von endlichem Typ ein direkter Summand ist, wobei wir Satz 31.1 auf geeignete endlichdimensionale G-Untervektorräume V anwenden wollen. Dazu müssen wir zunächst sicherstellen, dass jedes $f \in R$ in einem endlichdimensionalen G-Untervektorraum $V \subseteq R$ liegt. Es sei $G = \mathrm{Spek}(H)$ ein affines Gruppenschema zu einer endlich erzeugten K-Hopf-Algebra H. Die Operation von G auf $X = \mathrm{Spek}(R)$, dem Spektrum einer endlich erzeugten K-Algebra, ist äquivalent zu einem Ringhomomorphismus (der Kooperation)

$$N \colon\ R \longrightarrow H \otimes_K R$$

(mit bestimmten Eigenschaften). Für ein $f \in R$ kann man dabei

$$N(f) = \sum_{i=1}^{n} a_i \otimes f_i$$

mit $a_i \in H$ und $f_i \in R$ schreiben. Die Operation des K-Spektrums von H auf R ist folgendermaßen gegeben: Ein Gruppenelement $\sigma \in K-\text{Spek}\,(R)$, also ein K-Algebrahomomorphismus

$$\sigma\colon\ H \longrightarrow K$$

schickt eine Funktion f auf

$$f\sigma = \sum_{i=1}^{n} \sigma(a_i) \otimes f_i.$$

Es wird also die Hintereinanderschaltung

$$R \xrightarrow{N} H \otimes_K R \xrightarrow{\sigma\otimes \mathrm{Id}_R} K \otimes_K R \xrightarrow{\cong} R$$

betrachtet.

Lemma 31.2. *Es sei K ein Körper, G ein affines Gruppenschema über K und*

$$\nu\colon\ G \times X \longrightarrow X$$

eine K-algebraische Operation von G auf einem affinen Schema $X=\text{Spek}(R)$, wobei R eine kommutative K-Algebra sei. Dann liegt jedes $f \in R$ in einem endlichdimensionalen $G(K)$-invarianten K-Untervektorraum von R.

Beweis. Wir betrachten die zur Operation gehörige algebraische Situation, also den K-Algebrahomomorphismus

$$N\colon\ R \longrightarrow H \otimes_K R,$$

wobei H die Hopf-Algebra zu G sei. Es sei

$$N(f) = \sum_{i=1}^{n} a_i \otimes f_i$$

mit $a_i \in H$ und $f_i \in R$. Für jedes $\sigma \in G(K)$ ist

$$f\sigma = \sum_{i=1}^{n} \sigma(a_i) \otimes f_i = \sum_{i=1}^{n} \sigma(a_i) f_i,$$

d.h. diese liegen alle in dem von $f_1, \ldots, f_n$ erzeugten K-Untervektorraum von R. Der von all diesen $f\sigma$, $\sigma \in G(K)$, erzeugte Untervektorraum ist also $G(K)$-invariant und endlichdimensional. □

Satz 31.3. *Es sei K ein algebraisch abgeschlossener Körper, G eine linear reduktive Gruppe über K, die auf einer endlich erzeugten K-Algebra R algebraisch operiere. Dann ist $R^G \subseteq R$ ein direkter Summand.*

Beweis. Es sei $V \subseteq R$ ein endlichdimensionaler G-Untervektorraum. Nach Satz 31.1 (2) ist $V = V^G \oplus W$ mit einem G-Komplement, das überdies eindeutig bestimmt ist und für welches $(W^*)^G = 0$ gilt. Es ist sinnvoll, zuerst die Eindeutigkeit einer Reynolds-Abbildung nachzuweisen. Es sei

$$\Phi\colon\ R \longrightarrow R^G$$

eine Reynolds-Abbildung. Nach Lemma 31.2 gibt es zu jedem $f \in R$ einen endlichdimensionalen G-Untervektorraum $V \subseteq R$ mit $f \in V$. Wegen der G-Invarianz von Φ ist $\Phi(V) \subseteq V$ und die Einschränkung $\Phi|_{V^G}$ ist die Identität auf V^G. Ferner ist $\Phi(W) = 0$. Bei $u \in \Phi(W)$, $u \neq 0$, könnte man nämlich mit Hilfe einer K-linearen Abbildung

$$h\colon\ R^G \longrightarrow K$$

mit $h(u) \neq 0$ eine Linearform $\neq 0$ auf R, nämlich $h \circ \Phi$, angeben, die zu $(W^*)^G$ gehört. Dadurch ist Φ auf V eindeutig bestimmt und somit kann es maximal eine Reynolds-Abbildung geben. Zur Existenz. Wir wählen zu $f \in R$ gemäß Lemma 31.2 einen endlichdimensionalen G-Untervektorraum $V \subseteq R$ und setzen

$$\Phi(f) := \pi_V(f),$$

wobei

$$\pi_V\colon\ V \longrightarrow V^G$$

die Projektion von V auf V^G längs des G-Komplementes Wvon V^G in V bezeichnet. Dabei ist $\Phi(f)$ unabhängig von der Wahl von V. Zu einem anderen V' ist nämlich $\pi_{V'}|_{V\cap V'} = \pi_V|_{V\cap V'}$. Um dies zu zeigen kann man $V \subseteq V'$ annehmen. Aus $V' = (V')^G \oplus W'$ ergibt sich durch Schneiden mit V sofort eine Zerlegung von V, die wegen der Eindeutigkeit mit $V^G \oplus W$ übereinstimmen muss. Somit haben wir eine wohldefinierte K-lineare Abbildung

$$\Phi\colon\ R \longrightarrow R^G.$$

Zu $f \in R^G$ ist natürlich $f \in V^G$ (für einen gewählten Unterraum) und somit ist die Einschränkung von Φ auf R^G die Identität. Für ein Gruppenelement $\sigma \in G$ und $f \in R$ kann man $\Phi(f\sigma)$ mit dem gleichen Untervektorraum V berechnen. Es sei $f = (u, w)$ die Zerlegung von f in der direkten Zerlegung

$$V = V^G \oplus W.$$

Die Zerlegung von $f\sigma$ hat dann die Form (u, w'), da ja die Zerlegung die Gruppenoperation respektiert und die Gruppe in der ersten Komponente identisch operiert. Somit ist

$$\Phi(f\sigma) = \pi_V(f\sigma) = u = \pi_V(f) = \Phi(f),$$

und Φ ist in der Tat eine Reynolds-Abbildung. □

Satz 31.4. *Es sei K ein algebraisch abgeschlossener Körper, G eine linear reduktive Gruppe über K, die auf einem endlichdimensionalen K-Vektorraum V K-rational operiere. Dann ist der Invariantenring $K[V]^G$ eine endlich erzeugte K-Algebra.*

Beweis. Dies folgt aus Satz 31.3 und aus Korollar 12.7 (die Homogenitätsvoraussetzung ist erfüllt). □

Satz 31.5. *Es sei K ein algebraisch abgeschlossener Körper, G eine linear reduktive Gruppe über K, die auf einer endlich erzeugten K-Algebra R K-algebraisch operiere. Dann ist der Invariantenring R^G eine endlich erzeugte K-Algebra.*

Beweis. Es sei $f_1, \ldots, f_n$ ein K-Algebraerzeugendensystem von R. Nach Lemma 31.2 gibt es einen endlichdimensionalen K-Untervektorraum $V \subseteq R$, der G-invariant ist. Es sei $K[V]$ der zum Vektorraum V gehörende Polynomring, auf dem G linear operiert. Es ist

$$p\colon\ K[V] \longrightarrow R$$

ein surjektiver K-Algebrahomomorphismus, der mit den Operationen von G verträglich ist. Zu einem invarianten Element $f \in R^G$ gibt es ein $h \in K[V]$, das auf f abbildet. Wiederum nach Lemma 31.2 gibt es einen endlichdimensionalen G-invarianten Untervektorraum $U \subseteq K[V]$ mit $h \in U$. Dann ist $f \in p(U)$ ebenfalls G-invariant und nach Aufgabe 31.5, angewandt auf

$$p|_U\colon\ U \longrightarrow p(U)$$

gibt es auch ein G-invariantes $h' \in K[V]$, das auf f abbildet. Es ist also

$$K[V]^G \longrightarrow R^G$$

ebenfalls surjektiv. Nach Satz 31.4 ist $K[V]^G$ und somit R^G endlich erzeugt. □

31. Arbeitsblatt

Aufgabe 31.1. Es sei K ein Körper der Charakteristik $p > 0$. Zeige, dass die Gruppe $\mathbb{Z}/(p)$ nicht linear reduktiv über K ist.

Aufgabe 31.2. Es sei K ein Körper und es sei A eine $m \times n$-Matrix und B eine $n \times m$-Matrix über K. Zeige

$$\operatorname{Spur}(A \circ B) \;=\; \operatorname{Spur}(B \circ A)\,.$$

Aufgabe 31.3. Es sei K ein Körper und es seien V und W endlichdimensionale K-Vektorräume. Zeige, dass durch die Spur

$$\operatorname{Hom}_K(V,W) \times \operatorname{Hom}_K(W,V) \longrightarrow K,\ (A,B) \longmapsto \operatorname{Spur}(A \circ B)\,,$$

eine vollständige Dualität gestiftet wird, dass also $\operatorname{Hom}_K(V,W)$ und $\operatorname{Hom}_K(W,V)$ in natürlicher Weise dual zueinander sind.

Aufgabe 31.4. Es sei K ein algebraisch abgeschlossener Körper und G eine linear reduktive Gruppe über K, die auf einem endlichdimensionalen K-Vektorraum rational operiere. Zeige unter Betrachtung der homogenen Komponenten von $K[V]$ ohne Verwendung von Satz 31.1 und Lemma 31.2, dass $K[V]^G$ ein direkter Summand von $K[V]$ ist.

Aufgabe 31.5. Es sei G eine linear reduktive Gruppe über einem algebraisch abgeschlossenen Körper K, und es seien zwei rationale Darstellungen von G in die beiden endlichdimensionalen K-Vektorräume V und W gegeben. Es sei

$$\varphi\colon V \longrightarrow W$$

eine surjektive lineare Abbildung, die mit den Operationen verträglich sei. Zeige

$$\varphi(V^G) = W^G.$$

32. Vorlesung - Klassische Gruppen

Die klassischen Gruppen über $\mathbb{C}$

Wir möchten zeigen, dass über den komplexen Zahlen die klassischen linearen Gruppen linear reduktiv sind. Dies stimmt nicht in positiver Charakteristik, so dass man dafür keinen algebraischen Beweis erwarten kann. Im Gegenteil benutzt der Beweis maßtheoretische Methoden, die wir aber nicht vollständig vorstellen können.

Lemma 32.1. *Es sei K ein Körper und V ein endlichdimensionaler K-Vektorraum. Es sei G eine affin-algebraische Gruppe, die auf V K-rational operiere. Dann gelten folgende Aussagen.*

(1) *Für einen Vektor $v \in V$ und einen K-Untervektorraum $U \subseteq V$ ist*

$$\{g \in G |\, g(v) \in U\} \subseteq G$$

Zariski-abgeschlossen.

(2) *Zu einem K-Untervektorraum $U \subseteq V$ ist*

$$H = \{g \in G |\, g(U) \subseteq U\} \subseteq G$$

eine Zariski-abgeschlossene Untergruppe von G (also selbst eine lineare Gruppe).

Beweis. (1). Die Operation

$$G \times V \longrightarrow V$$

ist nach Voraussetzung ein K-Morphismus und somit ist insbesondere zu jedem $v \in V$ die induzierte Abbildung

$$\phi_v\colon G \longrightarrow V,\ g \longmapsto g(v),$$

ein Morphismus (ϕ_v ist die Hintereinanderschaltung von $G \to G \times V$, $g \mapsto (g, v)$, mit der Operationsabbildung). Da $U \subseteq V$ Zariski-abgeschlossen ist, ist auch das Urbild $\phi_v^{-1}(U)$ abgeschlossen. (2). Offenbar ist H eine Untergruppe von G. Es sei $v_1, \ldots, v_r$ eine Basis von U. Die Bedingung $g(U) \subseteq U$ ist äquivalent zu $g(v_i) \in U$ für $i = 1, \ldots, r$. Daher ist H der Durchschnitt von endlich vielen (nach (1)) Zariski-abgeschlossenen Mengen und somit selbst abgeschlossen. □

Wir möchten zeigen, dass die linearen Gruppen $\mathrm{GL}_n(\mathbb{C})$ und $\mathrm{SL}_n(\mathbb{C})$ über den komplexen Zahlen linear reduktiv sind. Dazu brauchen wir einige analytische Hilfsmittel (die Aussage gilt nicht in positiver Charakteristik), und zwar die Existenz des *Haarschen Maßes*. Dazu zitieren wir den folgenden maßtheoretischen Satz.

Satz 32.2. *Auf einer kompakten topologischen Gruppe G existiert ein Maß μ (auf der σ-Algebra der Borelmengen) mit den beiden folgenden Eigenschaften.*

(1) $\mu(T) = \mu(g(T))$ *für jede messbare Menge $T \subseteq G$.*
(2) *Es ist $\mu(G) = 1$.*

Das Maß ist durch diese beiden Eigenschaften eindeutig bestimmt.

Diese Eigenschaften heißen *Translationsinvarianz* und *Normierung*. Das Maß, dass gemäß diesem Satz in einer kompakten Gruppe existiert, heißt *Haarsches Maß*.

Beispiel 32.3. Auf der 1-Sphäre S^1 lässt sich das Haarsche Maß einfach direkt definieren. Für einen Kreisbogen $A \subseteq S^1$ zu einem Winkel α im Bogenmaß muss natürlich $\mu(A) = \alpha/2\pi$ sein. Das Haarsche Maß ist also das $1/2\pi$-fache des Bogenmaßes. Dieser Ansatz liefert nicht nur ein Maß für zusammenhängende Teilbögen, sondern für jede Borelmenge, indem man von der messbaren Bijektion

$$\varphi\colon\ [0, 2\pi] \longrightarrow S^1,\ t \longmapsto (\cos t\,,\, \sin t\,),$$

ausgeht und für eine Borelmenge $B \subseteq S^1$ das Haarsche Maß durch

$$\mu(B) = \frac{\lambda(\varphi^{-1}(B))}{2\pi}$$

definiert, wobei λ das eindimensionale Borel-Lebesgue-Maß bezeichnet.

Die Existenz des Haarschen Maßes bedeutet insbesondere, dass über G eine sinnvolle Integrationstheorie möglich ist. D.h. für stetige Funktionen

$$f\colon\ G \longrightarrow \mathbb{C}$$

ist das Integral

$$\int_G f d\mu$$

definiert. Die Translationsinvarianz führt zu

$$\int_G f d\mu \;=\; \int_G f\lambda_h d\mu \;=\; \int_G f\rho_h d\mu$$

für jedes Gruppenelement $h \in G$, aufgefasst als Links- oder als Rechtsmultiplikation $\lambda_h, \rho_h \colon G \to G$. Mit der Existenz des Haarschen Maßes kann man auch stetige Abbildungen von G in einen endlichdimensionalen $\mathbb{R}$-Vektorraum integrieren.

Satz 32.4. *Es sei G eine kompakte Gruppe und*

$$\rho \colon\; G \longrightarrow \mathrm{GL}\,(V)$$

eine stetige Darstellung auf dem endlichdimensionalen $\mathbb{C}$-Vektorraum V. Dann gibt es eine direkte Zerlegung von V in irreduzible Darstellungen.

Beweis. Wir zeigen, dass ein G-Untervektorraum $U \subseteq V$ ein G-Komplement besitzt, daraus folgt die Aussage wie Satz 30.7 aus Lemma 30.6. Auch der Beweis ist analog zu Satz 30.7. Es sei

$$\pi \colon\; V \longrightarrow U$$

eine lineare Projektion von V auf U. Zu $v \in V$ ist die Abbildung

$$G \longrightarrow V,\; g \longmapsto g(\pi(g^{-1}(v))),$$

stetig. Wir definieren

$$\psi(v) \;=\; \int_G g(\pi(g^{-1}(v)))d\mu.$$

Aufgrund der Linearität von g und der Linearität des Integrals ist ψ eine lineare Abbildung, deren Bild in U liegt, da dies für π gilt und da U G-invariant ist. Für $u \in U$ ist

$$\psi(u) \;=\; \int_G g(\pi(g^{-1}(u)))d\mu \;=\; \int_G g(g^{-1}(u))d\mu \;=\; \int_G u d\mu \;=\; u.$$

Also ist ψ ebenfalls eine lineare Projektion von V auf U. Für beliebige $h \in G$ und $v \in V$ ist aufgrund der Translationsinvarianz

$$\begin{aligned}
\psi(hv) &= \int_G g(\pi(g^{-1}(hv)))d\mu \\
&= \int_G (hg)(\pi((hg)^{-1}(hv)))d\mu \\
&= \int_G h\left(g(\pi(g^{-1}(v)))\right)d\mu \\
&= h\left(\int_G g(\pi(g^{-1}(v)))d\mu\right) \\
&= h\psi(v),
\end{aligned}$$

so dass ψ mit der Gruppenoperation verträglich ist. Also ist $\operatorname{kern}\psi$ nach Lemma 30.5 ein G-invarianter Untervektorraum und somit ein G-Komplement von U. $\square$

Der Satz von Maschke ist ein Spezialfall des vorstehenden Satzes, da man eine endliche Gruppe mit der diskreten Topologie versehen und zu einer kompakten Gruppe machen kann. Das Haarsche Maß ist dabei einfach das normierte Zählmaß.

Lemma 32.5. *Es sei G eine affin-algebraische Gruppe über $\mathbb{C}$ derart, dass es eine kompakte Untergruppe $K \subseteq G$ gibt, deren Zariski-Abschluss gleich G ist. Dann ist G linear reduktiv.*

Beweis. Wir zeigen, dass es zu jeder $\mathbb{C}$-rationalen Darstellung

$$\rho\colon\ G \longrightarrow \mathrm{GL}\,(V)$$

auf einem $\mathbb{C}$-Vektorraum V und einem G-Untervektorraum $U \subseteq V$ ein G-Komplement gibt. Die induzierte Darstellung

$$\rho\colon\ K \longrightarrow \mathrm{GL}\,(V)$$

ist stetig. Daher gibt es nach Satz 32.4 ein K-Komplement $W \subseteq V$. Wir betrachten

$$H := \{g \in G |\, g(W) = W\}\ .$$

Dies ist eine Untergruppe von G, die K umfasst. Nach Lemma 32.1 ist H Zariski-abgeschlossen und daher gleich G. □

Die linearen Gruppen

$$\mathrm{GL}_n(\mathbb{C})\,,\ \mathrm{SL}_n(\mathbb{C})\,,\ \mathrm{O}_n(\mathbb{C})\,,\ \mathrm{SO}_n(\mathbb{C})\,,\ \mathrm{Sp}_n\,(\mathbb{C})$$

nennt man auch die *klassischen Gruppen*.

Definition 32.6. Es sei K ein Körper und E_n die Einheitsmatrix der Länge n. Eine Matrix $M \in \mathrm{GL}_n(K)$ mit

$$M^{tr}M\ =\ E_n$$

heißt *orthogonale Matrix*. Die Menge aller orthogonalen Matrizen heißt *orthogonale Gruppe*, sie wird mit

$$\mathrm{O}_n(K)\ =\ \left\{M \in \mathrm{GL}_n(K) \,|\, M^{tr}M = E_n\right\}$$

bezeichnet.

Man beachte, dass dies bei $K = \mathbb{C}$ nicht die unitäre Gruppe ist. Die Gruppe, die aus allen speziellen orthogonalen Matrizen besteht, also die Determinante 1 besitzen, heißt *spezielle orthogonale Gruppe*.

Definition 32.7. Es sei K ein Körper und $I_m = \begin{pmatrix} 0 & -E_m \\ E_m & 0 \end{pmatrix} \in \mathrm{GL}_{2m}(K)$, wobei E_m die Einheitsmatrix der Länge m ist. Eine Matrix $S \in \mathrm{GL}_{2m}(K)$ mit

$$S^{tr}I_mS\ =\ I_m$$

heißt *symplektische Matrix*. Die Menge aller symplektischen Matrizen heißt *symplektische Gruppe*, sie wird mit

$$\mathrm{Sp}_{2m}(K) = \left\{S \in \mathrm{GL}_{2m}(K) \mid S^{tr} I_m S = I_m\right\}$$

bezeichnet.

Da die definierenden Bedingungen dieser Gruppen ein System aus algebraischen Gleichungen bilden, sind diese Gruppen affin-algebraisch, es handelt sich also um lineare Gruppen.

Satz 32.8. *Die klassischen Gruppen*

$$\mathrm{GL}_n(\mathbb{C})\,,\ \mathrm{SL}_n(\mathbb{C})\,,\ \mathrm{O}_n(\mathbb{C})\,,\ \mathrm{SO}_n(\mathbb{C})\,,\ \mathrm{Sp}_n(\mathbb{C})$$

besitzen Zariski-dichte kompakte Untergruppen.

Beweis. Wir skizzieren einen Beweis für die allgemeine lineare Gruppe $\mathrm{GL}_n(\mathbb{C})$. Sie enthält die unitäre Gruppe $\mathrm{U}_n(\mathbb{C})$ als Untergruppe, die nach Aufgabe 32.2 kompakt ist. Für $n = 1$ ist beispielsweise $\mathrm{GL}_1(\mathbb{C}) \cong \mathbb{C}^\times$ und $\mathrm{U}_1(\mathbb{C}) \cong S^1$, die S^1 ist eine kompakte Gruppe, deren Zariski-Abschluss ganz $\mathbb{C}^\times$ ist, da ein Polynom, das auf S^1 verschwindet, das Nullpolynom sein muss. Bei größerem n ist die Argumentation deutlich komplizierter.

Wir benutzen die Exponentialabbildung für Matrizen, also die Abbildung

$$\exp : \mathrm{Mat}_n(\mathbb{C}) \longrightarrow \mathrm{GL}_n(\mathbb{C}),$$

$$A \longmapsto \exp A := \sum_{k=0}^{\infty} \frac{1}{k!} A^k = E_n + A + \frac{1}{2}A^2 + \frac{1}{6}A^3 + \ldots.$$

Dabei bedeutet A^n die n-te Potenz der Matrix bezüglich der Matrizenmultiplikation. Man kann zeigen, dass die definierende Reihe gegen eine invertierbare Matrix konvergiert, so dass die Abbildung wohldefiniert ist und dass sie analytisch ist, also in jeder Koordinaten durch eine Potenzreihe in n^2 vielen komplexen Variablen gegeben ist. Insbesondere ist die Abbildung komplexdifferenzierbar. Ferner ist die Exponentialabbildung surjektiv.

Wir betrachten nun den Untervektorraum der schiefhermiteschen Matrizen, das sind diejenigen Matrizen $A = (w_{jk})_{1 \leq j,k \leq n}$ mit $w_{kj} = -\overline{w_{jk}}$. Das sind diejenigen Matrizen, die für beliebige Vektoren $x, y \in \mathbb{C}$ die Bedingung

$$\langle Ax, y\rangle = -\langle x, Ay\rangle$$

für das Standardskalarprodukt erfüllen. Wir behaupten, dass die schiefhermiteschen Matrizen unter der Exponentialabbildung auf unitäre Matrizen abgebildet werden. Sei also A eine schiefhermitesche Matrix. Aufgrund der eben formulierten Eigenschaft gilt für eine beliebige quadratische Matrix B und Vektoren $u, v \in \mathbb{C}^n$ die Gleichheit

$$\langle ABu, Bv\rangle = -\langle Bu, ABv\rangle\,.$$

Für $B = \exp(tA)$ mit einem beliebigen (reellen oder komplexen Parameter) t ergibt dies

$$\langle A\exp(tA)u, \exp(tA)v\rangle + \langle \exp(tA)u, A\exp(tA)v\rangle \ = \ 0.$$

Dieser Ausdruck ist aber die Ableitung der Abbildung

$$\mathbb{R} \longrightarrow \mathbb{C},\, t \longmapsto \langle \exp(tA)u, \exp(tA)v\rangle\,,$$

was man sieht, wenn man diese Abbildung als Hintereinanderschaltung

$$\mathbb{R} \longrightarrow \mathrm{Mat}_n(\mathbb{C}) \longrightarrow \mathbb{C}^n \times \mathbb{C}^n \longrightarrow \mathbb{C}$$

mit

$$t \longmapsto \exp(tA),\, C \longmapsto (Cu, Cv), \text{ und } (w,z) \longmapsto \langle w, z\rangle$$

schreibt. Daher ist $\langle \exp(tA)u, \exp(tA)v\rangle$ unabhängig von t und somit gleich $\langle u, v\rangle$, da dies der Wert für $t = 0$ ist. Also ist $\exp(tA)$ eine Isometrie für jedes t und insbesondere ist $\exp(A)$ eine Isometrie, also eine unitäre Matrix.

Wir müssen jetzt zeigen, dass der Zariski-Abschluss der unitären Gruppe gleich der allgemeinen lineare Gruppe ist. Dazu sei $f \in \mathbb{C}[X_{ij}]$ ein Polynom in n^2 Variablen, das auf der unitären Gruppe verschwindet. Es ist $f = 0$ zu zeigen. Wir betrachten die Verknüpfung $g = f \circ \exp$, die eine holomorphe Funktion auf $\mathrm{Mat}_n(\mathbb{C}) \cong \mathbb{C}^{n^2}$ ist. Wegen der erwähnten Surjektivität der Exponentialfunktion genügt es zu zeigen, dass $g = 0$ ist. Nach der Vorüberlegung verschwindet g auf dem reellen Untervektorraum der schiefhermiteschen Matrizen. Daher verschwindet auch die Ableitung $g'(P)$ auf diesem Untervektorraum für jeden Punkt P. Wir betrachten daher zuerst den Fall einer komplexen Linearform L auf $\mathrm{Mat}_n(\mathbb{C})$, die auf den schiefhermiteschen Matrizen verschwindet. Wir ersetzen die Variablen W_{ij} von $\mathrm{Mat}_n(\mathbb{C})$ durch $W_{jj}, W_{jk} - W_{kj}, W_{jk} + W_{kj}$ $(j \neq k)$. Die Bedingung schiefhermitesch bedeutet in diesen Variablen, dass die Imaginärteile von $W_{jk} - W_{kj}$ und dass die Realteile von $W_{jj}, W_{jk} + W_{kj}$ gleich 0 sind. Der Kern von L enthält also zu jedem Element u der transformierten Basis eine volle reelle Gerade $\mathbb{R}u$ und damit muss überhaupt u zum Kern gehören, d.h. $L = 0$. Dies bedeutet wiederum, dass $g'(P) = 0$ und daher ist g konstant, also $g = 0$. □

Satz 32.9. *Die klassischen Gruppen*

$$\mathrm{GL}_n(\mathbb{C})\,,\ \mathrm{SL}_n(\mathbb{C})\,,\ \mathrm{O}_n(\mathbb{C})\,,\ \mathrm{SO}_n(\mathbb{C})\,,\ \mathrm{Sp}_n\,(\mathbb{C})$$

sind linear reduktiv.

Beweis. Dies folgt aus Satz 32.8 und aus Lemma 32.5. □

32. Arbeitsblatt

Aufgabe 32.1. Finde eine kompakte Untergruppe innerhalb der komplexen invertierbaren Diagonalmatrizen.

Aufgabe 32.2. Zeige, dass die unitäre Gruppe $\mathrm{U}_n(\mathbb{C})$ (als Teilmenge des $\mathbb{C}^{n^2}$) abgeschlossenen und beschränkt, also kompakt ist.

Aufgabe 32.3. Zeige, dass die additive Gruppe $(\mathbb{C}, +, 0)$ keine kompakte Untergruppe enthält, die in der Zariski-Topologie dicht ist.

Aufgabe 32.4. Es sei $A \in \mathrm{Mat}_n(\mathbb{C})$ eine Matrix. Zeige, dass $\exp A$ in der $\mathbb{C}$-Unteralgebra $\mathbb{C}[A]$ liegt.

Aufgabe 32.5. Zeige, dass für vertauschbare Matrizen $A, B \in \mathrm{Mat}_n(\mathbb{C})$ die Beziehung

$$\exp(A \circ B) \ = \ (\exp\, A) \circ (\exp\, B)$$

gilt.

Aufgabe 32.6. Es sei $A \in \mathrm{Mat}_n(\mathbb{C})$ eine Matrix. Zeige, dass die Ableitung der Abbildung

$$\mathbb{C} \longrightarrow \mathrm{GL}_n(\mathbb{C}) \subseteq \mathrm{Mat}_n(\mathbb{C}),\, t \longmapsto \exp(tA),$$

gleich $A \circ \exp(tA)$ ist.

Aufgabe 32.7. Es sei $A \in \mathrm{Mat}_n(\mathbb{C})$ eine Matrix mit der Eigenschaft $\exp(tA) \in \mathrm{U}_n(\mathbb{C})$ für alle $t \in \mathbb{C}$. Zeige, dass A schiefhermitsch ist.

Aufgabe 32.8. Zeige, dass man auf die Exponentialabbildung

$$\exp : \ \mathrm{Mat}_n(\mathbb{C}) \longrightarrow \mathrm{GL}_n(\mathbb{C}) \subseteq \mathrm{Mat}_n(\mathbb{C}),\, A \longmapsto \exp\, A,$$

in der Nullmatrix den Satz über die Umkehrabbildung anwenden kann.

Anhang A: Bildlizenzen

Die Bilder dieses Textes stammen aus Commons (also http://commons.wikimedia.org), und stehen unter unterschiedlichen Lizenzen, die zwar alle die Verwendung hier erlauben, aber unterschiedliche Bedingungen an die Verwendung und Weitergabe stellen. Es folgt eine Auflistung der verwendeten Bilder dieses Textes (nach der Seitenzahl geordnet, von links nach rechts, von oben nach unten) zusammen mit ihren Quellen, Urhebern (Autoren) und Lizenzen. Dabei ist *Quelle* so zu verstehen, dass sich, wenn man

http://commons.wikimedia.org/wiki/File:

unmittelbar davor setzt, die entsprechende Datei auf Commons ergibt. *Autor* benennt den Urheber des Werkes, falls dieser bekannt ist. *Benutzer* meint den Hochlader der Datei; wenn keine weitere Information über den Autor vorliegt, so gilt der Benutzer als Urheber. Die Angabe des Benutzernamen ist so zu verstehen, dass sich, wenn man

http://commons.wikimedia.org/wiki/User:

unmittelbar davor setzt, die Benutzerseite ergibt. Wenn das Bild ursprünglich in einem anderen Wikimedia-Projekt hochgeladen wurde, so wird die Domäne (bspw. *de.wikipedia.org*) explizit angegeben.

Die *Lizenz* ist die auf der Dateiseite auf Commons angegebene Lizenz. Dabei bedeuten

- GFDL: Gnu Free Documentation License (siehe den angehängten Text, falls diese Lizenz vorkommt)
- CC-BY-SA-2.5 (3.0): Creative Commons Attribution ShareAlike 2.5 (oder 3.0)
- PD: gemeinfrei (public domain)

Abbildungsverzeichnis