Bachelorarbeit

Der Satz von Quillen-Suslin und Hermitesche Ringe

Betreuung
Prof. Dr. Jan Kohlhaase
Fakultät für Mathematik
Universität Duisburg-Essen

vorgelegt von:
Yogendra Puvanenthiran

Inhaltsverzeichnis

Einleitung

Satz von Quillen-Suslin
Sei R ein Hauptidealring und $n \in \mathbb{N}$. Dann ist jeder endlich erzeugte, projektive $R[t_1, \ldots, t_n]$-Modul frei.

Das Ziel dieser Bachelorarbeit ist es den Satz von Quillen-Suslin zu beweisen. Dafür dient Kapitel 1 als Vorbereitung, wo wir eine Aussage aus der homologischen Algebra beweisen und ein Hilfslemma, das als Beweis zur Noether-Normalisierung diente, verallgemeinern werden. In Kapitel 2 zeigen wir, dass jeder endlich erzeugte, projektive $R[t_1, \ldots, t_n]$-Modul M, mit R als Hauptidealring, stabil frei ist, d.h. es existiert ein endlich erzeugter, freier $R[t_1, \ldots, t_n]$-Modul N derart, dass $M \oplus N$ frei ist. Dafür konstruieren wir die Grothendieck-Gruppe eines Ringes und charakterisieren anhand dessen die stabile Freiheit. Wir gucken uns hierfür auch reguläre Ringe an. Weiter in Kapitel 3 zeigen wir, dass Polynomringe mit endlich vielen Variablen über Hauptidealringen hermitesch sind, d.h. stabil freie Moduln sind frei. Dies zeigen wir mit Hilfe der unimodularen Erweiterungseigenschaft eines Ringes. Wir setzen für diese Bachelorarbeit viele Begriffe und Erkenntnisse der kommutativen Algebra voraus. Bis auf Proposition 1.2 und Satz 1.10 werden wir alle Aussagen beweisen.

1 Grundlagen und Vorbereitung

In der gesamten Bachelorarbeit sei R ein kommutativer Ring mit Eins und n eine beliebige natürliche Zahl. Außerdem sei $\underline{n}$ die Menge der natürlichen Zahlen von 1 bis n.

1.1 Projektive Auflösung

Definition 1.1
Sei M ein R-Modul. Eine Auflösung von M ist eine exakte Sequenz von R-Moduln der Form

$$\ldots \to M_n \to M_{n-1} \to \ldots \to M_0 \to M \to 0.$$

Als Notation verwenden wir hierfür $M_* \to M$. Sei nun E eine Eigenschaft von R-Moduln (z.B. frei oder endlich erzeugt). Wir sagen ferner, M besitzt eine E Auflösung, falls alle R-Moduln M_i, in der obigen Sequenz, die Eigenschaft E besitzen. Eine Auflösung $M_* \to M$ heißt endlich, falls $M_n = 0$ für alle hinreichend großen n.

Proposition 1.2
Sei M ein R-Modul. Die folgenden Aussagen sind äquivalent:

(i) Für jede surjektive R-lineare Abbildung $g : N_1 \longrightarrow N_2$ und jede R-lineare Abbildung $f : M \longrightarrow N_2$ gibt es eine R-lineare Abbildung $f' : M \longrightarrow N_1$, sodass $g \circ f' = f$. Schematisch:

$$\begin{tikzcd} & M \arrow[d, "f"] \arrow[dl, dotted, "f'"'] \\ N_1 \arrow[r, "g"] & N_2 \end{tikzcd}$$

(ii) Jede exakte Sequenz von R-Moduln $0 \to N \to \tilde{M} \to M \to 0$ zerfällt, d.h. $\tilde{M} \cong M \oplus N$.

(iii) Es gibt einen R-Modul N, sodass $M \oplus N$ frei ist.

Beweis Wir verweisen hierbei auf [La06] Prop I.1.2 und Cor I.1.3. $\square$

Definition 1.3
Ein R-Modul M heißt projektiv, falls er die äquivalenten Bedingungen in Prop 1.2 erfüllt.

Korollar 1.4
Sei M ein endlich erzeugter, projektiver R-Modul. Dann existiert ein R-Modul N so, dass $M \oplus N$ endlich erzeugt und frei ist

Beweis
Sei $(m_i)_{i\in\underline{n}}$ ein Erzeugendensystem von M. Wir betrachten nun die R-lineare Abbildung $f : R^n \to M, e_i \mapsto m_i$, wobei $(e_i)_{i\in\underline{n}}$ die Standardbasis von R^n ist. Die folgende exakte Sequenz

$$0 \to \ker(f) \to R^n \to M \to 0$$

zerfällt aufgrund der Projektivität von M. Somit erhalten wir

$$M \oplus \ker(f) \cong R^n.$$

□

Das Ziel dieses Unterkapitels ist der Beweis des nachfolgenden Lemmas. Auf die Begriffe und Notationen gehen wir im Laufe des Kapitels ein.

Lemma 1.5
Sei $0 \to P \to Q \to M \to 0$ eine kurze exakte Sequenz von R-Moduln. Ferner seien $Q_* \to Q$ und $P_* \to P$ projektive Auflösungen. Dann besitzt M eine projektive Auflösung $M_* \to M$, für die eine exakte Sequenz

$$0 \to Q_* \to M_* \to P_*[-1] \to 0$$

existiert. Insbesondere gilt: Sind P_* und Q_* endlich, so auch M_*.

Für den Beweis benötigen wir etwas an Vorbereitung und unter anderem eine Einführung in Kettenkomplexe. Wir orientieren uns im folgenden Abschnitt an [Bo13] Kapitel 5.1.

Ein Kettenkomplex $\ldots \longrightarrow M_{i+1} \xrightarrow{d_{i+1}} M_i \xrightarrow{d_i} M_{i-1} \longrightarrow \ldots$ ist eine Sequenz von R-Moduln $(M_i)_{i\in\mathbb{Z}}$ mit R-linearen Abbildungen $d_i : M_i \to M_{i-1}$ für die gilt, dass $d_i \circ d_{i+1} = 0$ für alle $i \in \mathbb{Z}$. Zu dieser Bedingung ist auch äquivalent, dass $\mathrm{im}(d_{i+1}) \subseteq \ker(d_i)$. Als Notation verwenden wir hierfür (M_*, d), wobei mit M_* die Sequenz von R-Moduln $(M_i)_{i\in\mathbb{Z}}$ und d die Ansammlung der dazugehörigen R-linearen Abbildungen d_i gemeint ist. Wir nennen $\mathrm{H}_i(M_*) := \ker(d_i)/\mathrm{im}(d_{i+1})$ den i-ten Homologiemodul. Falls $\mathrm{H}_i(M_*) = 0$, so gilt $\ker(d_i) = \mathrm{im}(d_{i+1})$ und somit wäre ein Kettenkomplex an der Stelle i exakt. Ein Homomorphismus von Kettenkomplexen $f_* : M_* \longrightarrow N_*$ ist eine Ansammlung von R-linearen Abbildungen $f_i : M_i \longrightarrow N_i$, wobei das Diagramm

$$\begin{tikzcd} M_i \arrow[r, "d_i"] \arrow[d, "f_i"] & M_{i-1} \arrow[d, "f_{i-1}"] \\ N_i \arrow[r, "e_i"] & N_{i-1} \end{tikzcd}$$

für alle $i \in \mathbb{Z}$ kommutiert. Dies ermöglicht es uns Sequenzen von Kettenkomplexen zu betrachten. Eine Sequenz von Kettenkomplexen $0 \longrightarrow M'_* \xrightarrow{f_*} M_* \xrightarrow{g_*}$

$M''_* \longrightarrow 0$ ist exakt, falls für alle $i \in \mathbb{Z}$ die Sequenz $0 \longrightarrow M'_i \xrightarrow{f_i} M_i \xrightarrow{g_i} M''_i \longrightarrow 0$ exakt ist.

Proposition 1.6
Eine exakte Sequenz von Kettenkomplexen $0 \longrightarrow M'_* \xrightarrow{f_*} M_* \xrightarrow{g_*} M''_* \longrightarrow 0$ induziert eine lange exakte Sequenz von Homologiemoduln:

$$\ldots \longrightarrow \mathrm{H}_i(M'_*) \xrightarrow{\mathrm{H}_i(f_*)} \mathrm{H}_i(M_*) \xrightarrow{\mathrm{H}_i(g_*)} \mathrm{H}_i(M''_*) \longrightarrow \mathrm{H}_{i-1}(M'_*) \xrightarrow{\mathrm{H}_{i-1}(f_*)} \ldots$$

Beweis (vgl. [Bo13] Proposition 5.1.1)
Seien $(M, d), (M', d'), (M'', d'')$ Kettenkomplexe mit folgender exakten Sequenz

$$0 \longrightarrow M'_* \xrightarrow{f_*} M_* \xrightarrow{g_*} M''_* \longrightarrow 0 \ (\star).$$

Wir schränken, wegen $\mathrm{im}(d_i) \subseteq \ker(d_{i-1})$, die Bildmenge von $d_i : M_i \longrightarrow M_{i-1}$ auf $\ker(d_{i-1})$ ein. Nun wenden wir den Homomorphiesatz auf $\mathrm{im}(d_{i+1}) \subseteq \ker(d_i)$ an und erhalten eine eindeutige Abbildung $\tilde{d_i} : M_i/\mathrm{im}(d_{i+1}) \longrightarrow \ker(d_{i-1})$ mit den folgenden Eigenschaften:

(i) Es gilt $\tilde{d_i} = d_i \circ \pi$, wobei $\pi : M_i \longrightarrow M_i/\mathrm{im}(d_{i+1})$ die kanonische Projektion ist. Schematisch:

$$\begin{tikzcd} M_i \arrow[r, "d_i"] \arrow[d, "\pi"] & \ker(d_{i-1}) \\ M_i/\mathrm{im}(d_{i+1}) \arrow[ur, "\tilde{d}_i"] & \end{tikzcd}$$

(ii) $\ker(\tilde{d_i}) = \pi(\ker(d_i)) = \ker(d_i)/\mathrm{im}(d_{i+1}) = \mathrm{H}_i(M_*)$

(iii) $\mathrm{coker}(\tilde{d_i}) = \ker(d_{i-1})/\mathrm{im}(\tilde{d_i}) = \ker(d_{i-1})/\mathrm{im}(d_i) = \mathrm{H}_{i-1}(M_*)$

Ähnlich verfahren wir mit d'_i und d''_i. Wir betrachten nun das folgende Diagramm:

$$\begin{tikzcd} 0 \arrow[r] & M'_i \arrow[r, "f_i"] \arrow[d, "d'_i"] & M_i \arrow[r, "g_i"] \arrow[d, "d_i"] & M''_i \arrow[r] \arrow[d, "d''_i"] & 0 \\ 0 \arrow[r] & M'_{i-1} \arrow[r, "f_{i-1}"] & M_{i-1} \arrow[r, "g_{i-1}"] & M''_{i-1} \arrow[r] & 0 \end{tikzcd}$$

Da f_* und g_* Homomorphismen von Kettenkomplexen sind, kommutiert das Diagramm. Wegen $(\star)$ sind die Zeilen exakt. Durch Anwendung des Schlangenlemmas erhalten wir die exakte Sequenz

$$0 \to \ker(d'_i) \to \ker(d_i) \to \ker(d''_i) \to \mathrm{coker}(d'_i) \to \mathrm{coker}(d_i) \to \mathrm{coker}(d''_i) \to 0,$$

wobei die Exaktheit ganz außen aus der Injektivität von f_i bzw. der Surjektivität von g_i folgt. Wir betrachten die linke Hälfte dieser Sequenz für $i - 1$ und die rechte Hälfte für $i+1$. Diese werden durch die Abbildungen $\tilde{d}'_i$, $\tilde{d}_i$ und $\tilde{d}''_i$ zu einem kommutativen Diagramm

$$\begin{tikzcd}
& \operatorname{coker}(d'_{i+1}) \arrow[r] \arrow[d, "\tilde{d}'_i"] & \operatorname{coker}(d_{i+1}) \arrow[r] \arrow[d, "\tilde{d}_i"] & \operatorname{coker}(d''_{i+1}) \arrow[r] \arrow[d, "\tilde{d}''_{i-1}"] & 0 \\
0 \arrow[r] & \ker(d'_{i-1}) \arrow[r] & \ker(d_{i-1}) \arrow[r] & \ker(d''_{i-1}) &
\end{tikzcd}$$

verbunden. Wir wenden nun wieder das Schlangenlemma an und erhalten, unter Berücksichtigung, dass $\ker(\tilde{d}_i) = \mathrm{H}_i(M_*)$ und $\operatorname{coker}(\tilde{d}_i) = \mathrm{H}_{i-1}(M_*)$ gilt, die folgende, exakte Sequenz von Homologiemoduln

$$\mathrm{H}_i(M'_*) \longrightarrow \mathrm{H}_i(M_*) \longrightarrow \mathrm{H}_i(M''_*) \longrightarrow \mathrm{H}_{i-1}(M'_*) \longrightarrow \mathrm{H}_{i-1}(M_*) \longrightarrow \mathrm{H}_{i-1}(M''_*).$$

$\square$

Korollar 1.7
Sei $0 \to M_* \to M'_* \to M''_* \to 0$ eine exakte Sequenz von Kettenkomplexen. Falls zwei der Kettenkomplexe exakt sind, so ist auch der dritte Kettenkomplex exakt.

Beweis (vgl. [Bo13] Korollar 5.1.2)
Seien ohne Einschränkung die Kettenkomplexe M'_* und M''_* exakt, das heißt $\mathrm{H}_i(M'_*) = \mathrm{H}_i(M''_*) = 0$ für alle $i \in \mathbb{Z}$, so induziert die obige exakte Sequenz von Kettenkomplexen die folgende exakte Sequenz

$$\ldots \longrightarrow 0 \longrightarrow \mathrm{H}_i(M_*) \longrightarrow 0 \longrightarrow \ldots$$

Damit gilt auch $\mathrm{H}_i(M_*) = 0$. $\square$

Lemma 1.8
Seien $M_* \to M$ und $N_* \to N$ zwei Auflösungen von zwei R-Moduln M und N, wobei $M_* \to M$ projektiv sei. Ferner sei $f : M \longrightarrow N$ eine R-lineare Abbildung. Dann gibt es einen Homomorphismus von Kettenkomplexen $f_* : M_* \longrightarrow N_*$, sodass das Diagramm

$$\begin{tikzcd}
M_* \arrow[r] \arrow[d, "f_*"'] & M \arrow[d, "f"] \\
N_* \arrow[r] & N
\end{tikzcd}$$

kommutiert.

Beweis (vgl. [Bo13] Lemma 5.1.9 (i))
Wir betrachten das Diagramm

$$\begin{tikzcd}
\ldots \arrow[r] & M_2 \arrow[r, "d_2"] \arrow[d, "f_2"] & M_1 \arrow[r, "d_1"] \arrow[d, "f_1"] & M_0 \arrow[r, "d_0"] \arrow[d, "f_0"] & M \arrow[r] \arrow[d, "f"] & 0 \\
\ldots \arrow[r] & N_2 \arrow[r, "e_2"] & N_1 \arrow[r, "e_1"] & N_0 \arrow[r, "e_0"] & N \arrow[r] & 0.
\end{tikzcd}$$

M_0 ist projektiv und $e_0 : N_0 \longrightarrow N$ ist surjektiv. Daher erhalten wir, aufgrund von Proposition 1.2 (i), für $f \circ d_0 : M_0 \longrightarrow N$ eine R-lineare Abbildung

$$f_0 : M_0 \longrightarrow N_0 \text{ mit } e_0 \circ f_0 = f \circ d_0.$$

Um f_1 zu konstruieren, betrachten wir $f_0 \circ d_1 : M_1 \longrightarrow N_0$. Verketten wir dies links mit e_0 erhalten wir

$$e_0 \circ f_0 \circ d_1 = f \circ d_0 \circ d_1 = f \circ 0 = 0$$

und damit $\mathrm{im}(f_0 \circ d_1) \subseteq \ker(e_0) = \mathrm{im}(e_1)$. Aufgrund der Projektivität von M_1 erhalten wir für die surjektive Abbildung $e_1' : N_1 \longrightarrow \mathrm{im}(e_1), n_1 \longmapsto e_1(n_1)$ und $f_0 \circ d_1$, eine R-lineare Abbildung $f_1 : M_1 \longrightarrow N_1$ mit

$$e_1 \circ f_1 = e_1' \circ f_1 = f_0 \circ d_1.$$

Induktiv lassen sich so auch die restlichen f_i, für $i \in \mathbb{N}\backslash\{0, 1\}$, konstruieren. $\square$

Notation
Sei (M_*, d) ein Kettenkomplex und $k \in \mathbb{Z}$. $M[k]_*$ sei der Kettenkomplex mit R-Moduln $M[k]_i$, wobei $M[k]_i = M_{k+i}$ und R-linearen Abbildungen $d[k]_i$, wobei $d[k]_i = (-1)^k d_i$.

Jetzt können wir Lemma 1.5, mit den erarbeiteten Methoden, beweisen.

Beweis von Lemma 1.5
(vgl. [La06] Theorem II.5.7 (Beweisidee) und [Ro94] Definition 1.7.5)
Seien $(P_*, d) \to P$ und $(Q_*, e) \to Q$ projektive Auflösungen mit der exakten Sequenz

$$0 \longrightarrow P \xrightarrow{f} Q \xrightarrow{g} M \longrightarrow 0.$$

Nach Lemma 1.8 gibt es einen Homomorphismus von Kettenkomplexen $f_* : P_* \longrightarrow Q_*$, sodass das Diagramm

$$\begin{tikzcd} \dots \arrow[r] & P_2 \arrow[r, "d_2"] \arrow[d, "f_2"] & P_1 \arrow[r, "d_1"] \arrow[d, "f_1"] & P_0 \arrow[r, "d_0"] \arrow[d, "f_0"] & P \arrow[r] \arrow[d, "f"] & 0 \\ \dots \arrow[r] & Q_2 \arrow[r, "e_2"] & Q_1 \arrow[r, "e_1"] & Q_0 \arrow[r, "e_0"] & Q \arrow[r] & 0 \end{tikzcd} \qquad (\star)$$

kommutiert. Wir wollen nun anhand von P_* und Q_* einen Kettenkomplex (M_*, c) konstruieren. Dafür setzen wir $M_i := P_{i-1} \oplus Q_i$ und $c_i : M_i \longrightarrow M_{i-1}$ mit

$$c_i(p_{i-1}, q_i) := (-d_{i-1}(p_{i-1}), f_{i-1}(p_{i-1}) + e_i(q_i)).$$

Des Weiteren ist c_i R-linear und $\mathrm{im}(c_{i+1}) \subseteq \ker(c_i)$, da

$$\begin{aligned} c_i(c_{i+1}(p_i, q_{i+1})) &= c_i(-d_i(p_i), f_i(p_i) + e_{i+1}(q_{i+1})) \\ &= ((-d_{i-1} \circ d_i)(p_i), f_{i-1}(-d_i(p_i)) + e_i(f_i(p_i)) + (e_i \circ e_{i+1})(q_{i+1})) \\ &= (0, -f_{i-1}(d_i(p_i)) + e_i(f_i(p_i))) \\ &\overset{(\star)}{=} (0, -e_i(f_i(p_i) + e_i(f_i(p_i)))) = (0, 0) \end{aligned}$$

Das folgende Diagramm stellt diese Konstruktion zum Teil dar:

$$
\begin{tikzcd}
Q_* & \cdots \arrow[r] & Q_3 \arrow[r, "e_3"] \arrow[d] & Q_2 \arrow[r, "e_2"] \arrow[d] & Q_1 \arrow[r, "e_1"] \arrow[d] & Q_0 \arrow[r, "e_0"] & Q \arrow[r] & 0 \\
 & \cdots \arrow[r] & Q_3 \arrow[r, "e_3"] & Q_2 \arrow[r, "e_2"] & Q_1 \arrow[r, "e_1"] & Q_0 & & \\
M_* & & \oplus & \oplus & \oplus & & & \\
 & \cdots \arrow[r] & P_2 \arrow[r, "-d_2"] \arrow[uur, "f_2"] & P_1 \arrow[r, "-d_1"] \arrow[uur, "f_1"] & P_0 \arrow[uur, "f_0"] & & & \\
P_*[-1] & \cdots \arrow[r] & P_2 \arrow[r, "d_2"] \arrow[u] & P_1 \arrow[r, "d_1"] \arrow[u] & P_0 \arrow[r, "d_0"] \arrow[u] & P \arrow[r] & 0 &
\end{tikzcd}
$$

Nun erweitern wir M_* durch M und $c_0 := g \circ e_0 : M_0 \longrightarrow M$ zu einem Komplex $M_* \to M$ und betrachten das Diagramm

$$
\begin{tikzcd}
\cdots \arrow[r] & Q_1 \arrow[r, "e_1"] & Q_0 \arrow[r, "e_0"] \arrow[d, "id_{Q_0}"] & Q \arrow[r] \arrow[d, "g"] & 0 \\
\cdots \arrow[r] & M_1 \arrow[r, "c_1"] & M_0 = Q_0 \arrow[r, "c_0"] & M \arrow[r] & 0
\end{tikzcd}
$$

Da g und e_0 beide surjektiv sind, ist auch c_0 surjektiv. Es verbleibt noch zu zeigen, dass $M_* \to M$ tatsächlich eine projektive Auflösung ist. M_i ist projektiv, da dies eine direkte Summe aus den projektiven Moduln P_{i-1} und Q_i ist. Seien $G_* : Q_* \to M_*$ und $H_* : M_* \to P[-1]_*$ Homomorphismen von Kettenkomplexen gegeben durch

$$G_i : Q_i \longrightarrow P_{i-1} \oplus Q_i,\ q_i \mapsto (0, q_i) \text{ und } H_i : P_{i-1} \oplus Q_i \longrightarrow P_{i-1},\ (p_{i-1}, q_i) \mapsto p_{i-1}.$$

Offensichtlich ist G_i injektiv und H_i surjektiv. Da offenbar $\ker(H_i) = \operatorname{im}(G_i)$, ist die Sequenz

$$0 \longrightarrow Q_i \xrightarrow{G_i} M_i \xrightarrow{H_i} P_{i-1} \longrightarrow 0$$

für alle $i \in \mathbb{N} \backslash \{0\}$ exakt. Per Definition ist daher die Sequenz von Kettenkomplexen

$$0 \longrightarrow Q_* \xrightarrow{G_*} M_* \xrightarrow{H_*} P[-1]_* \longrightarrow 0$$

exakt. Q_* und $P[-1]_*$ sind nach unserer Voraussetzung exakt und nach Korollar 1.7 gilt, dass auch M_* exakt ist. Abschließend zeigen wir, dass die zweite Zeile im obigen Diagramm an der Stelle M_0 exakt ist, d.h. dass $\operatorname{im}(c_1) = \ker(c_0)$. Sei $a \in \operatorname{im}(c_1)$, dann gibt es $p_0 \in P_0$ und $q_1 \in Q_1$, sodass $e_1(q_1) + f_0(p_0) = a$. Unter Berücksichtigung von $(\star)$ und $\operatorname{im}(g) = \ker(f)$ haben wir

$$
\begin{aligned}
c_0(a) &= c_0(e_1(q_1)) + c_0(f_0(p_0)) \\
&= g(e_0 \circ e_1(q_1)) + g((e_0 \circ f_0)(p_0))) \\
&= g((f \circ d_0)(p_0)) = (g \circ f)(d_0(p_0)) = 0.
\end{aligned}
$$

Dies zeigt $a \in \ker(c_0)$. Sei umgekehrt $q_0 \in \ker(c_0)$, d.h. $(g \circ e_0)(q_0) = 0$. Daraus folgt nun, dass $e_0(q_0) \in \ker(g) = \operatorname{im}(f)$ und somit $f(p) = e_0(q_0)$ für ein $p \in P$.

Da $d_0 : P_0 \longrightarrow P$, aufgrund der Exaktheit von P_*, surjektiv ist, gibt es wiederum ein $p_0 \in P_0$ mit $d_0(p_0) = p$. Zusammen betrachtet ergibt sich

$$e_0(q_0) = f(p) = (f \circ d_0)(p_0) \overset{(\star)}{=} (e_0 \circ f_0)(p_0) = e_0(f_0(p_0)).$$

Daraus folgt aber nun, dass $q_0 - f_0(p_0) \in \ker(e_0) = \mathrm{im}(e_1)$, also existiert ein $q_1 \in Q_1$ mit $e_1(q_1) = q_0 - f_0(p_0)$. Nun ist

$$c_1(p_0, q_1) = f_0(p_0) + e_1(q_1) = f_0(p_0) + q_0 - f_0(p_0) = q_0.$$

Dies zeigt $q_0 \in \mathrm{im}(c_1)$ und somit die Exaktheit. □

Bemerkung
Den Kettenkomplex M_*, wie oben konstruiert, nennt man auch den Abbildungskegel von $f_* : P_* \longrightarrow Q_*$.

1.2 Normierte Polynome

Für den Beweis der Noether-Normalisierung verwendete man das folgende Lemma (vgl. [La06] S.102-103).

Lemma 1.9
Sei K ein Körper und $f(t_1, \dots, t_n) \in K[t_1, \dots, t_n] \backslash K$.
Dann gibt es $N \in \mathbb{N}$, $c \in K \backslash \{0\}$ und ein in t_1 normiertes Polynom $h \in K[t_1, \dots, t_n]$, sodass

$$f(t_1, t_2 + t_1^N, \dots, t_n + t_1^N) = c \cdot h(t_1, \dots, t_n).$$

Wir wollen dieses Lemma verallgemeinern. Dafür benötigen wir etwas an Vorbereitung.

Erinnerung
Sei $\mathfrak{p} \in \mathrm{Spec}(R) = \{\mathfrak{q} \subseteq R \mid \mathfrak{q} \text{ ist ein Primideal}\}$ und I ein Ideal in R. Wir sagen $\mathfrak{p}$ ist ein minimales Primideal über I, falls $I \subseteq \mathfrak{p}$ und für alle $\mathfrak{q} \in \mathrm{Spec}(R)$ mit $I \subseteq \mathfrak{q} \subseteq \mathfrak{p}$ stets $\mathfrak{p} = \mathfrak{q}$ folgt. Des Weiteren ist

$$\mathrm{ht}(\mathfrak{p}) = \sup\{n \in \mathbb{N} \mid \text{es gibt Primideale } \mathfrak{p}_0, \dots, \mathfrak{p}_\mathfrak{n}, \text{ sodass } \mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_\mathfrak{n} = \mathfrak{p}\}$$

die Höhe von $\mathfrak{p}$ und

$$\mathrm{ht}(I) = \min_{\mathfrak{q} \in \mathrm{Spec}(R) \text{ mit } I \subseteq \mathfrak{q}} \{\mathrm{ht}(\mathfrak{q})\}$$

die Höhe von I.

Satz 1.10 (Krull'scher Dimensionssatz)
Sei R ein noetherscher Ring und $I \subseteq R$ ein Ideal mit Erzeugendensystem $r_1, \dots, r_n$.

Dann gilt für jedes minimale Primideal $\mathfrak{p}$ über I die Abschätzung $\operatorname{ht}\mathfrak{p} \leq n$. Ist umgekehrt $m := \operatorname{ht}(\mathfrak{p})$, so existiert ein von m Elementen erzeugtes Ideal $J \subseteq R$, sodass $\mathfrak{p}$ minimal über J ist.

Beweis Wir verweisen auf [Bo13] Theorem 2.4.6 und Lemma 2.4.10. □

Proposition 1.11
Sei R ein noetherscher Ring, $\mathfrak{q} \in \operatorname{Spec}(R[t])$ und $\mathfrak{p} = \mathfrak{q} \cap R \in \operatorname{Spec}(R)$. Dann gilt

$$\operatorname{ht}(\mathfrak{q}) = \begin{cases} \operatorname{ht}(\mathfrak{p}) & \mathfrak{q} = \mathfrak{p}R[t] \\ \operatorname{ht}(\mathfrak{p}) + 1 & \mathfrak{q} \supsetneq \mathfrak{p}R[t]. \end{cases}$$

Beweis (vgl. [La06] Proposition II.7.7)
Jede Primidealkette $\mathfrak{p}_0 \subsetneq \ldots \subsetneq \mathfrak{p}_n = \mathfrak{p}$ der Länge n wird zu

$$\mathfrak{p}_0 R[t] \subsetneq \ldots \subseteq \mathfrak{p}_n R[t] = \mathfrak{p}R[t] \subseteq \mathfrak{q}$$

erweitert. Somit haben wir

$$\operatorname{ht}(\mathfrak{q}) \geq \begin{cases} \operatorname{ht}(\mathfrak{p}) & \mathfrak{q} = \mathfrak{p}R[t] \\ \operatorname{ht}(\mathfrak{p}) + 1 & \mathfrak{q} \supsetneq \mathfrak{p}R[t]. \end{cases}$$

Sei jetzt $\operatorname{ht}(\mathfrak{p}) = n$ und $\mathfrak{p}$ minimal über einem Ideal $I \subseteq R$, welches von n Elementen erzeugt wird (vgl. Satz 1.10). Dann ist auch $\mathfrak{p}R[t]$ minimal über $IR[t]$, weil aus $IR[t] \subseteq \mathfrak{q}' \subseteq \mathfrak{p}R[t]$, für $\mathfrak{q}' \in \operatorname{Spec}(R[t])$, stets $I \subseteq \mathfrak{q}' \cap R \subseteq \mathfrak{p}$ folgt und somit gilt $\mathfrak{q}' \cap R = \mathfrak{p}$. Daraus folgt aber $\mathfrak{p}R[t] \subseteq \mathfrak{q}'$ und damit $\mathfrak{q}' = \mathfrak{p}R[t]$. Nach Satz 1.10 ist nun $\operatorname{ht}(\mathfrak{p}[t]) \leq n$. Falls $\mathfrak{q} = \mathfrak{p}R[t]$, so erhalten wir $\operatorname{ht}(\mathfrak{q}) = \operatorname{ht}(\mathfrak{p})$. Sei daher also $\mathfrak{q} \supsetneq \mathfrak{p}R[t]$ und betrachte $f \in \mathfrak{q} \backslash \mathfrak{p}R[t]$. Es reicht nun aus zu zeigen, dass $\mathfrak{q}$ minimal über $J := IR[t] + \operatorname{span}_{R[t]}(f)$ ist, denn J wird von den Elementen $r_1, \ldots, r_n, f$ erzeugt und nach Satz 1.10 gilt dann

$$\operatorname{ht}(\mathfrak{q}) \leq n + 1 = \operatorname{ht}(\mathfrak{p}) + 1.$$

Sei dafür $\mathfrak{q}' \in \operatorname{Spec}(R[t])$ mit $J \subseteq \mathfrak{q}' \subseteq \mathfrak{q}$. Dann haben wir

$$I \subseteq J \cap R \subseteq \mathfrak{q}' \cap R \subseteq \mathfrak{q} \cap R = \mathfrak{p}$$

und daher gilt $\mathfrak{q}' \cap R = \mathfrak{p}$. Sei nun $T := R/\mathfrak{p}$ und TS^{-1} die Lokalisierung von T an $S := (R/\mathfrak{p}) \backslash \{0\}$, d.h. TS^{-1} ist der Quotientenkörper von $R/\mathfrak{p}$. Des Weiteren ist $\mathfrak{p}R[t] \subsetneq \mathfrak{q}' \subseteq \mathfrak{q}$ und wir erhalten aus $0 \neq \mathfrak{q}'/(\mathfrak{p}R[t]) \subseteq \mathfrak{q}/(\mathfrak{p}R[t])$ die Primidealkette $(\mathfrak{q}'/(\mathfrak{p}R[t]))S^{-1} \subseteq (\mathfrak{q}/(\mathfrak{p}R[t]))S^{-1}$, da $\mathfrak{q}'/(\mathfrak{p}R[t]) \cap S = \emptyset = \mathfrak{q}/(\imath R[t]) \cap S$ gilt. Jedoch ist die Krulldimension von $TS^{-1}[t]$ gleich 1 und somit gilt bereits

$$(\mathfrak{q}'/(\mathfrak{p}R[t]))S^{-1} = (\mathfrak{q}/(\mathfrak{p}R[t]))S^{-1}.$$

Die vom kanonischen Ringhomomorphismus $T[t] \to T[t]S^{-1} \cong TS^{-1}[t]$ induzierte Abbildung $\operatorname{Spec}(T[t]S^{-1}) \to \operatorname{Spec}(T[t])$ liefert uns $\mathfrak{q}'/(\mathfrak{p}R[t]) = \mathfrak{q}/(\mathfrak{p}R[t])$. Daraus folgt $\mathfrak{q}' = \mathfrak{q}$, wie gewünscht. □

Notation
Sei I ein Ideal in $R[t]$. Wir setzen

$$\mathrm{H}(I) := \{r \in R \mid \exists f \in I \text{ mit } f(t) = r \cdot t^n + \sum_{i=0}^{n-1} r_i t^i\}.$$

$\mathrm{H}(I)$ enthält alle Höchstkoeffizienten der Polynome in I. Zudem gilt stets $I \cap R \subseteq \mathrm{H}(I)$. Offenbar ist $\mathrm{H}(I) \subseteq R$ ein Ideal.

Lemma 1.12
Sei R ein noetherscher Ring und $I \subseteq R[t]$ ein Ideal. Dann gilt

$$\mathrm{ht}(\mathrm{H}(I)) \geq \mathrm{ht}(I).$$

Beweis (vgl. [La06] Lemma III.3.2)
Sei $\mathfrak{q} \in \mathrm{Spec}(R[t])$ und setze $\mathfrak{p} := \mathfrak{q} \cap R$. Es gilt $\mathfrak{p} \subseteq \mathrm{H}(\mathfrak{q})$. Falls $\mathfrak{q} = \mathfrak{p}R[t]$, so ist $\mathrm{H}(\mathfrak{q}) = \mathfrak{p}$, da die Koeffizienten eines Polynomes von $\mathfrak{q}$ in $\mathfrak{p}$ liegen. Mit Proposition 1.11 erhalten wir

$$\mathrm{ht}(\mathrm{H}(\mathfrak{q})) = \mathrm{ht}(\mathfrak{p}) = \mathrm{ht}(\mathfrak{q}).$$

Falls nun $\mathfrak{p}R[t] \subsetneq \mathfrak{q}$, so ist auch $\mathfrak{p} \subsetneq \mathrm{H}(\mathfrak{q})$. Andernfalls wäre für $f(t) = r \cdot t^n + \sum_{i=0}^{n-1} r_i \cdot t^i \in \mathfrak{q}$ stets $r \in \mathfrak{p}$ und damit $f(t) - r \cdot t^n = \sum_{i=0}^{n-1} r_i \cdot t^i \in \mathfrak{q}$. Induktiv würde man $r, r_{n-1}, \ldots, r_0 \in \mathfrak{p}$ erhalten und daraus $f \in \mathfrak{p}R[t]$ für alle $f \in \mathfrak{q}$, d.h. $\mathfrak{p}R[t] = \mathfrak{q}$. Das ist ein Widerspruch. Wieder nach Proposition 1.11 haben wir nun

$$\mathrm{ht}(\mathrm{H}(\mathfrak{q})) > \mathrm{ht}(\mathfrak{p}) = \mathrm{ht}(\mathfrak{q}) - 1, \text{ also } \mathrm{ht}(\mathrm{H}(\mathfrak{q})) \geq \mathrm{ht}(\mathfrak{q}).$$

Sei nun I ein beliebiges Ideal in $R[t]$. Für $I = R[t]$ erhalten wir $\mathrm{H}(I) = R$ und somit $\mathrm{ht}(I) = \infty = \mathrm{ht}(\mathrm{H}(I))$. Daher schließen wir im Folgenden das Einsideal aus. Seien $\mathfrak{q}_1, \ldots, \mathfrak{q}_m$ die minimalen Primideale über I und betrachte nun

$$\prod_{i=1}^{m} \mathfrak{q}_i \subseteq \bigcap_{i=1}^{m} \mathfrak{q}_i = \mathrm{Rad}(I) = \{r \in R[t] \mid \exists\ n \in \mathbb{N} \text{ mit } r^n \in I\}.$$

Die erste Inklusion ist klar und die zweite Gleichung ist Hilberts Nullstellensatz. Für beliebige Ideale $I_1, I_2 \subseteq R[t]$ gilt stets $\mathrm{H}(I_1) \cdot \mathrm{H}(I_2) \subseteq H(I_1 \cdot I_2)$, da das Produkt der beiden Höchstkoeffizienten von $g_1 \in I_1$ und $g_2 \in I_2$ wieder ein Höchstkoeffizient von $g_1 \cdot g_2 \in I_1 \cdot I_2$ oder gleich 0 ist. Für geeignetes $n \in \mathbb{N}$ ist $(\prod_{i=1}^{m} \mathfrak{q}_i)^n \subseteq I$, da dass Ideal $\prod_{i=1}^{m} \mathfrak{q}_i$ endlich erzeugt ist. Dadurch erhalten wir

$$\prod_{i=1}^{m} \mathrm{H}(\mathfrak{q}_i)^n \subseteq \mathrm{H}((\prod_{i=1}^{m} \mathfrak{q}_i)^n) \subseteq \mathrm{H}(I).$$

Sei nun $\mathfrak{p}$ ein Primideal, welches $\mathrm{H}(I)$ enthält und $\mathrm{ht}(\mathfrak{p}) = \mathrm{ht}(\mathrm{H}(I))$ erfüllt. Eines der Ideale $\mathrm{H}(\mathfrak{q}_i)$ liegt, aufgrund der Primidealeigenschaft auch vollständig in $\mathfrak{p}$, denn anderenfalls existieren für $i \in \underline{m}$ stets $q_i \in \mathrm{H}(\mathfrak{q}_i) \backslash \mathfrak{p}$. Wegen $\prod_{i=1}^{m} q_i^m \in \prod_{i=1}^{m} \mathrm{H}(\mathfrak{q}_i)^n \subseteq \mathfrak{p}$ steht dies im Widerspruch dazu, dass $\mathfrak{p}$ ein Primideal ist. Dadurch erhalten wir

$$\mathrm{ht}(I) \leq \mathrm{ht}(\mathfrak{q}_i) \leq \mathrm{ht}(\mathrm{H}(\mathfrak{q}_i)) \leq \mathrm{ht}(\mathfrak{p}) = \mathrm{ht}(\mathrm{H}(I)).$$

□

Nun können wir eine verallgemeinerte Form von Lemma 1.9 beweisen.

Satz 1.13
Sei R ein noetherscher Ring endlicher Krulldimension d und $S = R[t_1, \dots, t_n]$ der Polynomring über R mit n Variablen. Ferner sei $I \subseteq S$ ein Ideal mit $\mathrm{ht}(I) > d$. Dann gibt es Variablen $s_1, \dots, s_n \in S$, sodass $S = R[s_1, \dots, s_n]$ und I enthält ein in s_1 normiertes Polynom.

Beweis (vgl. [La06] Theorem III.3.3)
Wir zeigen diese Aussage per Induktion über die Anzahl der Variablen. Für $n = 0$ ist $I = R$, womit nichts zu zeigen ist. Die Aussage gelte nun für $S = R[t_1, \dots, t_n]$ mit $n \in \mathbb{N}\backslash\{0\}$. Wir zeigen diese Aussage nun für $T := R[t_1, \dots, t_{n+1}]$. Sei nun $I \subseteq T$ ein Ideal mit $\mathrm{ht}(I) > d$. Da $T = S[t_{n+1}]$ betrachten wir $\mathrm{H}(I) \subseteq S$ und nach Lemma 1.12 ist $\mathrm{ht}(\mathrm{H}(I)) \geq \mathrm{ht}(I) > d$. Nach unserer Annahme gilt $S = R[s_1, \dots, s_n]$ für geeignete Variablen $s_1, \dots, s_n \in S$ und $\mathrm{H}(I)$ enthält ein in s_1 normiertes Polynom

$$g = s_1^k + \sum_{i=0}^{k-1} g_i \cdot s_1^i \text{ mit } g_i \in R[s_2, \dots, s_n].$$

Wegen $g \in \mathrm{H}(I)$, enthält I ein Polynom

$$f = g \cdot t_{n+1}^m + \sum_{i=0}^{m-1} h_i \cdot t_{n+1}^i \text{ mit } h_i \in S.$$

Sei nun $\deg_{s_1}$ der Grad eines Polynomes in der Variable s_1 und setze

$$M := \max_{i \in \underline{m-1}} \deg_{s_1}(h_i).$$

Des Weiteren setzen wir

$$s_{n+1} := t_{n+1} - s_1^N \text{ für ein } N \in \mathbb{N} \text{ (welches wir unten festlegen)}$$

Somit erhalten wir

$$T = S[t_{n+1}] = R[s_1, \dots, s_n][s_{n+1} + s_1^N] = R[s_1, \dots, s_{n+1}]$$

Es bleibt noch zu zeigen, dass f bei geeigneter Wahl von N normiert ist. Für

$$g \cdot t_{n+1}^m = (s_1^k + \sum_{i=0}^{k-1} g_i \cdot s_1^i) \cdot (s_{n+1} + s_1^N)^m$$

gilt $\deg_{s_1}(g \cdot t_{n+1}^m) = k + N \cdot m$ und für den Restterm

$$h := \sum_{i=0}^{m-1} h_i \cdot t_{n+1}^i = \sum_{i=0}^{m-1} h_i \cdot (s_{n+1} + s_1^N)^i$$

von f haben wir die Abschätzung $\deg_{s_1}(h) \leq M + N \cdot (m-1)$. Nun wählen wir N so, dass

$$\deg_{s_1}(g \cdot t_{n+1}^m) = k + N \cdot m > M + N \cdot (m-1) \geq \deg_{s_1}(h).$$

Aufgrund der Normiertheit von $g \cdot t_{n+1}$ in s_1 und der Wahl von N, ist f in s_1 normiert. $\square$

2 Stabil freie Moduln

Definition 2.1
Ein R-Modul M heißt stabil frei, falls ein endlich erzeugter, freier R-Modul F existiert, sodass der R-Modul $M \oplus F$ frei ist.

In diesem Kapitel zeigen wir, dass jeder endlich erzeugte, projektive $R[t_1, \ldots, t_n]$-Modul, mit R als Hauptidealring, stabil frei ist.

Bemerkung
Die Bedingung, dass F endlich erzeugt sein muss, ist notwendig. Denn falls nicht, so wäre jeder projektive R-Modul M stabil frei. Wähle dazu einen R-Modul N sodass $M \oplus N$ frei ist. Dann ist $F := \oplus_{i=1}^{\infty}(M \oplus N)$ frei mit

$$M \oplus F = M \oplus \bigoplus_{i=1}^{\infty}(M \oplus N) \cong M \oplus \bigoplus_{i=1}^{\infty}(N \oplus M) \cong (M \oplus N) \oplus \ldots \cong \bigoplus_{i=1}^{\infty}(M \oplus N) = F$$

Natürlich ist jeder stabil freie Modul projektiv. Manchmal ist er sogar frei:

Proposition 2.2
Jeder stabil freie, nicht endlich erzeugte R-Modul M ist frei.

Beweis (vgl. [La06] Proposition I.4.2)
Sei M nicht endlich erzeugt und stabil frei, d.h. es gibt einen endlich erzeugten, freien R-Modul F, sodass $M \oplus F =: N$ frei ist. Sei $(e_i)_{i \in I}$ eine Basis von N. Da M nicht endlich erzeugt ist, ist I eine unendliche Indexmenge. Wir betrachten nun die kanonische Projektion $\pi_F : M \oplus F \to F$, $(m, f) \mapsto f$ und setzen

$$\tilde{M} := \ker(\pi_F) = \{(m, 0_F) | m \in M\} \cong M.$$

Da F endlich erzeugt ist, existiert wegen $F = \pi_F(M \oplus F) = \operatorname{span}_R(e_i)_{i \in I}$ eine endliche Teilmenge $I_0 \subseteq I$, sodass $\pi_F(\operatorname{span}_R(e_i)_{i \in I_0}) = F$. Zur Vereinfachung setzen wir $F' := \operatorname{span}_R(e_i)_{i \in I_0}$. Nun gibt es zu $(m, f) \in M \oplus F$ ein $(m', f') \in F'$, sodass $\pi_F((m', f')) = \pi_F((m, f))$ und somit $(m', f') - (m, f) \in \ker(\pi_F)$. Daraus folgt nun, dass

$$M \oplus F = N = F' + \ker(\pi_F) = F' + \tilde{M}.$$

N/F' ist frei, da dieser isomorph zu $\operatorname{span}_R((e_i)_{i \in I \setminus I_0})$ ist und $(e_i)_{i \in I \setminus I_0}$ linear unabhängig ist. Nach dem Isomorphiesatz gilt nun

$$N/F' \cong (F' + \tilde{M})/F' \cong \tilde{M}/(\tilde{M} \cap F').$$

Da $\tilde{M}/(\tilde{M} \cap F')$ frei, aber nicht endlich erzeugt ist, kann dieser Modul als direkte Summe von F und einem freien Modul M'' geschrieben werden. Daher ergibt sich

$$M \cong \tilde{M} \cong (\tilde{M} \cap F') \oplus \tilde{M}/(\tilde{M} \cap F') \cong (\tilde{M} \cap F') \oplus F \oplus M'' \cong F' \oplus M''.$$

□

Für einen R-Modul M sei (M) seine Isomorphieklasse, d.h. (M) ist die Ansammlung aller zu M isomorphen R-Moduln. Die Menge

$$\mathcal{P}(R) := \{(M) \mid M \text{ ist ein endlich erzeugter, projektiver } R\text{-Modul}\}$$

bildet zusammen mit der Verknüpfung $\oplus$ ein kommutatives Monoid. Das neutrale Element ist die Isomorphieklasse des Nullmoduls. $\mathcal{P}(R)$ ist im Allgemeinen keine Gruppe, doch wir können diese zu einer Gruppe „erweitern". Dazu benötigen wir den folgenden Satz.

Satz 2.3 (Grothendieck-Gruppe)
Sei H eine abelsche Halbgruppe, dann existiert eine abelsche Gruppe $\mathcal{G}(H)$ zusammen mit einem Halbgruppenhomomorphismus $\psi : H \to \mathcal{G}(H)$ und der folgenden universellen Eigenschaft:
Falls G eine weitere Gruppe und $\varphi : H \to G$ ein Halbgruppenhomomorphismus ist, so gibt es genau einen Gruppenhomomorphismus $\varphi' : \mathcal{G}(H) \to G$ mit $\varphi = \varphi' \circ \psi$.
Schematisch sieht das folgendermaßen aus:

$$\begin{tikzcd} H \arrow[r, "\psi"] \arrow[dr, "\varphi"'] & \mathcal{G}(H) \arrow[d, dotted, "\exists!\, \varphi' : \varphi' \circ \psi = \varphi"] \\ & G \end{tikzcd}$$

Bemerkung
Man nennt $\mathcal{G}(H)$ die Grothendieck-Gruppe von H oder auch die Gruppenvervollständigung von H.

Beweis (vgl. [Ro94] Theorem 1.1.3)
Sei H bezüglich $*$ eine abelsche Halbgruppe. Die Relation $\sim$ auf $H \times H$ sei definiert als

$$(h_1, h_2) \sim (h_1', h_2') \Leftrightarrow \exists\, g \in H, \text{ sodass } h_1 * h_2' * g = h_1' * h_2 * g.$$

Dies ist eine Äquivalenzrelation. Für die Reflexivität und die Symmetrie verwenden wir die Kommutativität von H. Für die Transitivität seien $(h_1, h_2), (h_1', h_2')$, $(h_1'', h_2'') \in H \times H$ mit $(h_1, h_2) \sim (h_1', h_2'), (h_1', h_2') \sim (h_1'', h_2'')$, d.h. es gibt $g_1, g_2 \in H$, sodass

$$h_1 * h_2' * g_1 = h_1' * h_2 * g_1 \text{ und } h_1' * h_2'' * g_2 = h_1'' * h_2' * g_2.$$

Wir betrachten nun

$$\begin{aligned} h_1 * h_2'' * (h_1' * g_2 * g_1) &= h_1 * h_2' * h_1'' * g_2 * g_1 && (H \text{ abelsch und } (h_1', h_2') \sim (h_1'', h_2'')) \\ &= h_2 * h_1' * h_1'' * g_2 * g_1 && (H \text{ abelsch und } (h_1, h_2) \sim (h_1', h_2')) \\ &= h_2 * h_1'' * (h_1' * g_2 * g_1). \end{aligned}$$

Daher erhalten wir $(h_1, h_2) \sim (h_1'', h_2'')$. Wir setzen nun

$$\mathcal{G}(H) := H \times H/\sim \text{ und } [(h_1, h_2)] := \{(h_1', h_2') \in H \times H \mid (h_1, h_2) \sim (h_1', h_2')\}.$$

Die Verknüpfung $*$ auf $\mathcal{G}(H)$ sei definiert durch

$$[(h_1, h_2)] * [(h_1', h_2')] = [(h_1 * h_1', h_2 * h_2')].$$

Nun zeigen wir, dass $\mathcal{G}(H)$ bezüglich $*$ eine wohldefinierte, abelsche Gruppe ist. Für die Wohldefiniertheit, seien $[(h_1, h_2)] = [(g_1, g_2)]$ und $[(h_1', h_2')] = [(g_1', g_2')]$, also gibt es $a, b \in H$, sodass $h_1 * g_2 * a = g_1 * h_2 * a$ und $h_1' * g_2' * b = g_1' * h_2' * b$. Nun gilt

$$\begin{aligned}(h_1 * h_1') * (g_2 * g_2') * (a * b) &= (h_1 * g_2 * a) * (h_1' * g_2' * b)\\ &= (g_1 * h_2 * a) * (g_1' * h_2' * b)\\ &= (g_1 * g_1') * (h_2 * h_2') * (a * b)\end{aligned}$$

und daraus folgt

$$[(h_1 * h_1', h_2 * h_2')] = [(g_1 * g_1'), (g_2 * g_2')].$$

Die Assoziativität und die Kommutativität von $\mathcal{G}(H)$ folgen aus denen von H. Für das neutrale Element beachten wir zunächst, dass für $g, h \in H$ gilt $[(h, h)] = [(g, g)]$, weil $h * g * a = g * h * a$ für ein beliebiges $a \in H$ erfüllt ist. Das neutrale Element von $\mathcal{G}(H)$ ist $[(h, h)]$, denn

$$[(h, h)] * [(h_1, h_2)] = [(h * h_1, h * h_2)] = [(h_1, h_2)].$$

Für $[(h_1, h_2)]$ ist $[(h_2, h_1)]$ das inverse Element, weil

$$[(h_1, h_2)] * [(h_2, h_1)] = [(h_1 * h_2, h_1 * h_2)].$$

Den Halbgruppenhomomorphismus $\psi : H \to \mathcal{G}(H)$ definieren wir als $\psi(h) = [(h^2, h)]$. Das ψ tatsächlich ein Homomorphismus ist, folgt aus

$$\begin{aligned}\psi(h_1 * h_2) &= [(h_1 * h_2)^2, h_1 * h_2]\\ &= [h_1^2 * h_2^2, h_1 * h_2] = [h_1^2, h_1] * [h_2^2, h_2]\\ &= \psi(h_1) * \psi(h_2).\end{aligned}$$

Für ψ gilt zudem noch

$$\begin{aligned}[h_1, h_2] &= [(h_1 * (h_1 * h_2), h_2 * (h_1 * h_2)]\\ &= [(h_1^2 * h_2, h_2^2 * h_1)] = [(h_1^2 * h_1)] * [(h_2, h_2^2)]\\ &= \psi(h_1) * \psi(h_2)^{-1}.\end{aligned}$$

Nun zeigen wir die universelle Eigenschaft. Sei nun $(G, \cdot)$ eine Gruppe und $\varphi : H \to G$ ein Halbgruppenhomomorphismus. Wir definieren nun den Gruppenhomomorphismus $\varphi' : \mathcal{G}(H) \to G$ durch

$$\varphi'([h_1, h_2]) := \varphi(h_1) \cdot \varphi(h_2)^{-1}.$$

Aufgrund der Definition von φ' erhalten wir $\varphi' \circ \psi = \varphi$. Die Homomorphismuseigenschaften folgen aus denen von φ. Es bleibt nur noch die Eindeutigkeit zu zeigen. Dafür betrachten wir einen weiteren Gruppenhomomorphismus $\phi : \mathcal{G}(H) \to G$ mit $\phi \circ \psi = \varphi$. Dann gilt

$$\begin{aligned}
\phi([(h_1, h_2)]) &= \phi([(h_1 * h_1 * h_2, h_1 * h_2 * h_1)]) \\
&= \phi([(h_1^2 * h_2, h_2^2 * h_1)]) \\
&= \phi([(h_1^2, h_1)]) * \phi([(h_2, h_2^2)]) \\
&= \phi(\psi(h_1)) \cdot \phi(\psi(h_2)^{-1}) \\
&= \varphi([h_1, h_2]) \\
&= \varphi'(\psi(h_1)) \cdot \varphi'(\psi(h_2)^{-1}) \\
&= \varphi'([(h_1, h_2]).
\end{aligned}$$

Da $[(h_1, h_2)] \in \mathcal{G}(H)$ beliebig war, folgt $\phi = \varphi'$, womit die Eindeutigkeit gezeigt ist.

□

Nach diesem Satz, gibt es für $\mathcal{P}(R)$ nun eine Gruppenvervollständigung $\mathcal{G}(\mathcal{P}(R))$. Diese bezeichnen wir als $K_0(R)$ und die Verknüpfung der Einfachheit halber als $+$. Außerdem setzen wir: $[M] := \psi((M))$, wobei $\psi : \mathcal{P}(R) \to K_0(R)$ der Halbgruppenhomomorphismus im Sinne von Satz 2.3 ist.

Lemma 2.4
Sei $0 \to M_1 \to M_2 \to \ldots \to M_n \to 0$ eine exakte Sequenz von endlich erzeugten, projektiven R-Moduln. Dann gilt in $K_0(R)$ die Gleichung

$$\sum_{j=1}^{n} (-1)^j [M_j] = [0].$$

Beweis (vgl. [Ro94] Lemma 3.1.10)
Wir zeigen dies per Induktion und beginnen mit $n = 3$. Nach Proposition 1.2 gilt $M_1 \oplus M_3 \cong M_2$ und somit

$$[M_1] - [M_2] + [M_3] = [M_1 \oplus M_3] - [M_2] = [M_2] - [M_2] = [0].$$

Kommen wir nun zum Induktionsschritt. Die exakte Sequenz

$$0 \to M_1 \to M_2 \to \ldots \to M_{n+1} \to 0$$

lässt sich in zwei Sequenzen unterteilen

$$0 \to N \to M_n \to M_{n+1} \to 0$$

$$0 \to M_1 \to \ldots \to M_{n-1} \to N \to 0,$$

wobei $N := \ker(M_n \to M_{n+1})$. Nun ist aufgrund der Projektivität von M_n und M_{n+1} auch N projektiv, weil $M_n \cong N \oplus M_{n+1}$. Nach Induktionsanfang und Induktionsvoraussetzung erhalten wir daher

$$[N] - [M_n] + [M_{n+1}] = [0] \text{ und } \sum_{j=1}^{n-1} (-1)^j [M_j] + (-1)^n [N] = [0]$$

Zusammen gesetzt ergibt sich

$$(-1)^n [N] - (-1)^n [M_n] + (-1)^n [M_{n+1}] = \sum_{j=1}^{n-1} (-1)^j [M_j] + (-1)^n [N].$$

Wenn wir jetzt die linke Seite nach [0] umformen, erhalten wir wie gewünscht

$$\sum_{j=1}^{n+1} (-1)^j [M_i] = [0].$$

□

Lemma 2.5
Sei M ein endlich erzeugter, projektiver R-Modul. Dann sind folgende Aussagen äquivalent:

(i) P ist stabil frei.

(ii) $[P] \in \mathbb{Z}[R]$, d.h. es gibt ein $a \in \mathbb{Z}$, sodass $[P] = a[R]$.

Beweis (vgl. [La06] Korollar I.6.2)
Sei M stabil frei, d.h. es gibt einen endlich erzeugten, freien R-Modul N, sodass $M \oplus N$ frei ist. Auch $M \oplus N$ ist endlich erzeugt und somit für ein $n \in \mathbb{N}$ isomorph zu R^n. Es gilt nun

$$\begin{aligned} [M] &= [M] + [N] - [N] \\ &= [M \oplus N] - [N] = [R^n] - [R^m] \\ &= n \cdot [R] - m \cdot [R] = (n - m) \cdot [R] \in \mathbb{Z}[R]. \end{aligned}$$

Sei nun umgekehrt $a \in \mathbb{Z}$ mit $[M] = a \cdot [R]$. Wähle $b \in \mathbb{N}$, sodass $a + b \geq 0$. Dann ist

$$[M \oplus R^b] = a \cdot [R] + b \cdot [R] = [R^{a+b}].$$

Da die Äquivalenzklassen gleich sind, gibt es nach Definition der Relation $\sim$ in der Konstruktion von $K_0(R)$ einen endlich erzeugten, projektiven R-Modul N, sodass

$$M \oplus R^b \oplus N \cong R^{a+b} \oplus N.$$

Dann gibt es wiederum einen endlich erzeugten R-Modul N', sodass $N \oplus N' =: N''$ frei ist, wobei dann auch N'' endlich erzeugt ist. Dann zeigt

$$M \oplus R^b \oplus N'' \cong R^{a+b} \oplus N'',$$

dass M stabil frei ist. □

Satz 2.6
Sei M ein endlich erzeugter, projektiver R-Modul. Die folgenden Aussagen sind äquivalent:

(i) M ist stabil frei.

(ii) M besitzt eine endliche Auflösung durch endlich erzeugte, stabil freie Moduln.

Beweis (vgl. [La06] Korollar I.6.3)
Sei M stabil frei und N ein endlich erzeugter, freier R-Modul, sodass $M \oplus N$ frei ist. Wir erhalten nun die exakte Sequenz

$$0 \to N \to M \oplus N \twoheadrightarrow M \to 0.$$

Für die Rückrichtung zeigen wir, aufgrund von Lemma 2.5, dass $[M] \in \mathbb{Z}[R]$. Sei daher

$$0 \to M_n \to \ldots \to M_1 \to M \to 0$$

eine endliche Auflösung durch endlich erzeugte stabil freie Moduln. Nach Lemma 2.4 erhalten wir

$$\sum_{i=1}^{n}(-1)^i[M_i] = (-1)^{n+1}[M].$$

Da alle M_i endlich erzeugt und stabil frei sind, ist $\sum_{i=1}^{n}[M_i]$ nach Lemma 2.5 ein Element von $\mathbb{Z}[R]$ und daher auch M. $\square$

Bemerkung
Der Beweis zeigt, dass man in Satz 2.6 (ii) die Bedingung „stabil frei“ auch durch „frei“ ersetzen kann.

Definition 2.7
Sei M ein $R[t]$-Modul. M ist von R erweitert, falls ein R-Modul M' existiert, sodass $R[t] \otimes_R M'$ isomorph zu M ist.

Bemerkung
Seien M und M' wie oben. Wenn M' als R-Modul endlich erzeugt, projektiv, stabil frei oder frei ist, so hat auch M als $R[t]$-Modul die entsprechende Eigenschaft.

Lemma von Swan 2.8
Sei R ein noetherscher Ring, N ein endlich erzeugter, von R erweiterter $R[t]$-Modul und M ein $R[t]$-Untermodul von N. Dann gibt es endlich erzeugte, von R erweiterte $R[t]$-Moduln P und Q, die zusammen mit M eine kurze exakte Sequenz der Form

$$0 \longrightarrow P \longrightarrow Q \longrightarrow M \longrightarrow 0$$

bilden.

Beweis (vgl. [La06] Lemma II.5.1)
Sei N_0 ein R-Modul mit $N = R[t] \otimes_R N_0$. Wegen $N/tN \cong N_0$ und da N als $R[t]$-Modul endlich erzeugt ist, ist N_0 als R-Modul endlich erzeugt. Wir setzen nun $N_l := \sum_{i=0}^{l} t^i \cdot R \otimes_R N_0$ und $M_l := M \cap N_l$. Falls $n_l \in N_l$, so ist $t \cdot n_l \in N_{l+1}$. Da N_0 endlich erzeugt ist, sind auch alle N_k, als R-Moduln und M, als $R[t]$-Modul endlich erzeugt, da $R[t]$ nach dem Hilberts Basissatz noethersch ist. Wir wählen k so groß, dass N_{k+1} und damit $M_{k+1} = N_{k+1} \cap M$ ein Erzeugendensystem von M enthält und setzen

$$P := R[t] \otimes_R M_k \text{ und } Q := R[t] \otimes_R M_{k+1}.$$

Wir definieren die $R[t]$-linearen Abbildungen $f : Q \longrightarrow M$ und $g : P \longrightarrow Q$ durch

$$f(t^n \otimes m) = t^n \cdot m \text{ und } g(t^n \otimes m) = t^{n+1} \otimes m - t^n \otimes t \cdot m.$$

Nun zeigen wir, dass die Sequenz

$$0 \longrightarrow P \xrightarrow{g} Q \xrightarrow{f} M \longrightarrow 0$$

exakt ist. Die Surjektivität von f folgt aus der Tatsache, dass $M_{k+1} \subseteq \mathrm{im}(f)$ und somit enthält $\mathrm{im}(f)$ ein Erzeugendensystem von M. Bevor wir zu der Injektivität von g übergehen, beachten wir zunächst, dass als R-Moduln

$$P = R[t] \otimes_R M_k \cong \bigoplus_{n \in \mathbb{N}} R \otimes_R M_k \cong \bigoplus_{n \in \mathbb{N}} M_k,$$

wobei $\sum_{i \in \mathbb{N}} t^i \otimes m_i$ auf $(m_i)_{i \in \mathbb{N}}$ abgebildet wird. Falls nun $\sum_{i=0}^{n} t^i \otimes m_i = 0$, so gilt $m_i = 0$, für alle $i \in \underline{n}$. Es bedeutet auch, falls $m \in M_k \backslash \{0\}$, so gilt für ein beliebiges $m' \in M_k$ stets $t^n \otimes m + t^{n-1} \otimes m' \neq 0$. Sei nun $p \in P \backslash \{0\}$ mit $p = \sum_{i=0}^{n} t^i \otimes m_i$, wobei $m_i \in M$ und $m_n \neq 0$. Dann gilt

$$g(p) = \sum_{i=0}^{n} t^{i+1} \otimes m_i - t^i \otimes t \cdot m_i = t^{n+1} \otimes m_n + \sum_{i=0}^{n} t^i \otimes (t \cdot m_i - m_{i+1}) \neq 0.$$

Dies zeigt, dass $\ker(g) = \{0\}$ und somit die Injektivität von g. Schließlich zeigen wir nun, dass $\ker(f) = \mathrm{im}(g)$. Es gilt dabei stets

$$f(g(t^n \otimes m)) = f(t^{n+1} \otimes m - t^n \otimes t \cdot m) = t^{n+1} \cdot m - t^{n+1} \cdot m = 0.$$

Sei jetzt $q = \sum_{i=0}^{n} t^i \otimes m_i \in \ker(f)$ mit $m_i \in M_{k+1}$. Wir zeigen nun per Induktion nach n, dass $q \in \mathrm{im}(g)$. Für $n = 0$ gilt $f(1 \otimes m) = 1 \cdot m = m = 0$. Die Aussage gelte für $n \in \mathbb{N} \backslash \{0\}$, d.h. ist $q' = \sum_{i=0}^{n} t^i \otimes m_i' \in \ker(f)$ so auch $q' \in \mathrm{im}(g)$. Sei jetzt $q = \sum_{i=0}^{n+1} t^i \otimes m_i$ mit $m_i = \sum_{j=0}^{k+1} t^j \otimes a_{ij}$ und $a_{ij} \in N_0$. Dann haben wir

$$\begin{aligned} 0 = f(q) = \sum_{i=0}^{n+1} t^i \cdot m_i &= \sum_{i=0}^{n+1} \sum_{j=0}^{k+1} t^{i+j} \otimes a_{ij} \\ &= t^{n+1+k+1} \otimes a_{n+1,k+1} + \sum_{j=0}^{k} t^{n+1+j} \otimes a_{n+1,j} + \sum_{i=0}^{n} \sum_{j=0}^{k+1} t^i \otimes a_{ij}. \end{aligned}$$

Wie oben, folgt hieraus, dass $a_{n+1,k+1} = 0$ gilt und somit $m_{n+1} \in M_k$. Jetzt haben wir

$$\begin{aligned} 0 &= f(q) - f(g(t^n \otimes m_{n+1})) = f(q - g(t^n \otimes m_{n+1})) \\ &= f(\sum_{i=0}^{n+1} t^i \otimes m_i - t^{n+1} \otimes m_{n+1} + t^n \otimes t \cdot m_{n+1}) \\ &= f(\sum_{i=0}^{n} t^i \otimes m_i + t^n \otimes t \cdot m_{n+1}). \end{aligned}$$

Nach unserer Induktionsbehauptung liegt daher auch $q - g(t^n \otimes m_{n+1})$ in $\operatorname{im}(g)$ und somit auch q, da $q - g(t^n \otimes m_{n+1}) + g(t^n \otimes m_{n+1}) \in \operatorname{im}(g)$. □

Definition 2.9
Ein Ring R heißt regulär, falls er folgende Bedingungen erfüllt:

(i) R ist noethersch.

(ii) Jeder endlich erzeugte R-Modul M besitzt eine endliche Auflösung durch endlich erzeugte projektive R-Moduln.

Satz von Swan 2.10
Sei R ein regulärer Ring. Dann gibt es für jeden endlich erzeugten $R[t_1, \ldots, t_n]$-Modul M eine endliche Auflösung durch Moduln der Form $R[t_1, \ldots, t_n] \otimes_R N$ mit N endlich erzeugt und projektiv über R.

Bemerkung
Aus dem obigen Satz und Hilberts Basissatz folgt unmittelbar:
Ist R regulär, so ist auch $R[t_1, \ldots, t_n]$ regulär.

Beweis (vgl. [La06] Theorem II.5.7)
Wir zeigen dies für $R[t]$ und induktiv folgt das dann auch für $R[t_1, \ldots, t_n]$.
Sei $(m_i)_{i \in \underline{n}}$ ein Erzeugendensystem von M. Wir betrachten die R-lineare Abbildung φ: $R[t]^n \longrightarrow M$, $e_i \mapsto m_i$, wobei $(e_i)_{i \in n}$ die Standardbasis von $R[t]^n$ ist und setzen $M' := \ker(\varphi)$. Dann erhalten wir die kurze exakte Sequenz

$$0 \longrightarrow M' \longrightarrow R[t]^n \xrightarrow{\varphi} M \longrightarrow 0.$$

Nun konstruieren wir eine von R erweiterte, endliche, projektive Auflösung für M' von der gewünschten Form. $R[t]^n$ ist offensichtlich ein von R erweiterter, endlich erzeugter $R[t]$-Modul und da M' ein endlich erzeugter Untermodul von $R[t]^n$ ist, können wir Lemma 2.8 anwenden und erhalten eine kurze exakte Sequenz

$$0 \longrightarrow P \xrightarrow{g} Q \xrightarrow{f} M' \longrightarrow 0,$$

wobei $P = R[t] \otimes_R P'$ und $Q = R[t] \otimes_R Q'$ von R erweiterte, endlich erzeugte $R[t]$-Moduln sind. Somit sind auch die R-Moduln P' und Q' endlich erzeugt. Da

R regulär ist, gibt es für P' und Q' jeweils eine endliche projektive Auflösung

$$0 \longrightarrow P'_n \longrightarrow \ldots \longrightarrow P'_0 \longrightarrow P' \longrightarrow 0$$
$$0 \longrightarrow Q'_m \longrightarrow \ldots \longrightarrow Q'_0 \longrightarrow Q' \longrightarrow 0.$$

Da $R[t]$ flach über R ist, sind auch die Sequenzen

$$0 \longrightarrow P_n \longrightarrow \ldots \longrightarrow P_0 \longrightarrow P \longrightarrow 0$$
$$0 \longrightarrow Q_m \longrightarrow \ldots \longrightarrow Q_0 \longrightarrow Q \longrightarrow 0$$

exakt, wobei $P_i = R[t] \otimes_R P'_i$ für alle $i \in \underline{n}$ und $Q_j = R[t] \otimes_R Q'_j$ für alle $j \in \underline{m}$ projektiv und damit insbesondere von R erweitert sind. Nun folgt aus Lemma 1.5, dass M' eine projektive, von R erweiterte Auflösung besitzt und somit auch M. □

Satz 2.11
Sei R ein regulärer Ring mit der Eigenschaft, dass jeder endlich erzeugte, projektive R-Modul stabil frei ist. Dann besitzt auch $R[t_1, \ldots, t_n]$ diese Eigenschaft.

Beweis (vgl. Beweisidee [La06] II.5.8)
Auch hier zeigen wir dies nur für $R[t]$ und gehen dann induktiv vor. Sei M ein endlich erzeugter, projektiver $R[t]$-Modul. Nach Satz 2.10 gibt es für M eine projektive Auflösung der Form

$$0 \longrightarrow R[t] \otimes_R M_m \longrightarrow \ldots \longrightarrow R[t] \otimes_R M_0 \longrightarrow M \longrightarrow 0,$$

wobei M_i für alle $i \in \{0, \ldots, m\}$ endlich erzeugt und projektiv über R ist. Nach unserer Voraussetzung sind alle M_i stabil frei über R. Daher ist $R[t] \otimes_R M_i$ stabil frei über $R[t]$. Nach Satz 2.6 ist M stabil frei über $R[t]$. □

Lemma 2.12
Jeder Hauptidealring R ist regulär.

Beweis
Da jeder Hauptidealring noethersch ist, verbleibt nur noch zu zeigen, dass ein endlich erzeugter R-Modul M eine endliche Auflösung durch endlich erzeugte projektive (und damit freie) R-Moduln besitzt. Sei dafür $(m_i)_{i \in \underline{n}}$ ein Erzeugendensystem von M. Die R-lineare Abbildung $\varphi : R^n \to M, e_i \mapsto m_i$, wobei $(e_i)_{i \in \underline{n}}$ die Standardbasis von R^n beschreibt, ist surjektiv. Als Untermodul von R^n ist $\ker(\varphi)$, nach dem Elementarteilersatz, frei. Damit konstruieren wir eine kurze exakte Sequenz

$$0 \longrightarrow \ker(\varphi) \longrightarrow R^n \xrightarrow{\varphi} M \longrightarrow 0.$$

□

Satz von Serre 2.13
Sei R ein Hauptidealring. Dann ist jeder endlich erzeugte, projektive $R[t_1, \ldots, t_n]$-Modul stabil frei.

Beweis
Projektive Moduln über einem Hauptidealring sind frei und daher auch stabil frei. Der Rest folgt aus Satz 2.11 und Lemma 2.12. □

3 Hermitesche Ringe

Definition 3.1
Ein Ring R heißt hermitesch, falls jeder stabil freie R-Modul frei ist.

Wir wollen nun zeigen, dass stabil freie $R[t_1, \dots, t_n]$-Moduln, mit R als Hauptidealring, frei sind oder anders formuliert: $R[t_1, \dots, t_n]$ ist hermitesch.

Definition 3.2
Sei $n \in \mathbb{N}$.

(i) Ein Element $(f_1, \dots, f_n) \in R^n$ heißt unimodular, falls $\operatorname{span}_R(f_1, \dots, f_n) = \sum_{i=1}^n f_i R = R$, d.h. falls $f_1, \dots, f_n$ das Einsideal erzeugen.

(ii) R hat die unimodulare Erweiterungseigenschaft, falls für alle $m \in \mathbb{N}$ jeder unimodulare Vektor $(f_1, \dots, f_m) \in R^m$ zu einer R-Basis von R^m ergänzt werden kann. Dies ist auch äquivalent dazu, dass es eine invertierbare Matrix $A \in \mathrm{GL}_m(R)$, gibt mit erster Spalte $(f_1, \dots, f_m)^t$.

Einen Zusammenhang zwischen hermitesch und unimodularer Erweiterungsschaft liefert der folgende Satz.

Satz 3.3
Sei R ein Ring mit der unimodularen Erweiterungseigenschaft. Dann ist R hermitesch.

Beweis (vgl. für Hinlänglichkeit [La02] Theorem XXI.3.6)
Sei M stabil frei und N ein endlich erzeugter, freier R-Modul, sodass $M \oplus N$ frei ist. Für ein geeignetes $n \in \mathbb{N}$ ist daher $N \cong R^n$. Wir zeigen nun die Aussage per Induktion nach n. Für $n = 1$ gilt nun, dass $M \oplus R$ frei ist. Wir nehmen an, dass M endlich erzeugt ist, denn ansonsten wäre M bereits nach Proposition 2.2 frei. Somit ist $M \oplus R$ isomorph zu R^m für ein $m \in \mathbb{N}$. Sei $f : M \oplus R \to R^m$ solch ein Isomorphismus, $\pi : M \oplus R \to R$ die Projektion auf die zweite Komponente und $g := \pi \circ f^{-1} : R^m \to R$. Da g surjektiv ist, existiert $a_1 \in R^m$ mit $g(a_1) = 1$, d.h. $f^{-1}(a_1) = (m_1, 1)$ für ein $m_1 \in M$. Der Vektor $a_1 := (a_{11}, \dots, a_{1m})$ ist unimodular, denn

$$1 = g(a_1) = g(\sum_{j=1}^m a_{1j} \cdot e_j) = \sum_{j=1}^m a_{1j} \cdot g(e_j) \in \sum_{j=1}^m R \cdot a_{ij}.$$

Nach Voraussetzung lässt sich a_1 zu einer Basis $(a_1, \dots, a_m)$ von R^m ergänzen. Wir schreiben $f^{-1}(a_j) = (m_j, r_j)$ mit $m_j \in M$ und $r_j \in R$ für $2 \leq j \leq m$. Dann ist mit $b_j := a_j - r_j \cdot a_1$ die Familie $(a_1, b_2, \dots, b_m)$ noch immer eine R-Basis von R^m mit

$$f^{-1}(b_j) = f^{-1}(a_j - r_j \cdot a_1) = (m_j, r_j) - r_j \cdot (m_1, 1) = (m_j - r_j \cdot m_1, 0) \in M \subseteq M \oplus R.$$

Ist $(m,0) \in M \subseteq M \oplus R$, so existieren $\lambda_1, \dots, \lambda_m \in R$ mit

$$(m,0) = \lambda_1 \cdot f^{-1}(a_1) + \sum_{j=2}^{m} \lambda_j \cdot f^{-1}(b_j) = (\lambda_1 \cdot m_1, \lambda_1) + (\sum_{j=2}^{m} \lambda_j (m_j - r_j \cdot m_1), 0),$$

woraus $\lambda_1 = 0$ folgt. Damit ist $(f^{-1}(b_j))_{2 \leq j \leq m}$ ein linear unabhängiges Erzeugendensystem von $M \subseteq M \oplus R$, d.h. M ist frei. Nun gelte die Aussage für ein $n \in \mathbb{N}$, d.h. ist M' stabil frei und $M' \oplus R^n$ frei, dann ist M' ebenfalls frei. Für $M \oplus R^{n+1} \cong M \oplus R \oplus R^n$ folgt, dass $M \oplus R$ frei ist und nach obiger Argumentation folgt wiederum, dass M frei ist.

□

Nach dem Elementarteilersatz ist jeder Hauptidealring R hermitesch nach obigem Satz besitzt er auch die unimodulare Erweiterungseigenschaft. Ziel des restlichen Kapitels ist es zu zeigen, dass auch $R[t_1, \dots, t_n]$ diese Eigenschaft besitzt.

Definition 3.4
Sei $f, g \in R^n$. Die Relation $\sim_R$ sei gegeben durch

$$f \sim_R g \Leftrightarrow \text{ es gibt ein } A \in GL_n(R), \text{ sodass } f = g \cdot A.$$

Aus den Eigenschaften einer invertierbaren Matrix folgt unmittelbar, dass $\sim_R$ eine Äquivalenzrelation ist.

Bemerkungen
Sei $f = (f_1, \dots, f_n) \in R^n$.

- Sei weiter $i < j \in \underline{n}$ und $r \in R$ mit

  $$f' := (f_1, \dots, f_j, \dots, f_i, \dots, f_n) \text{ und } f'' := (f_1, \dots, f_i + r \cdot f_j, \dots, f_n).$$

  Dann gilt, dass
  $$f \sim_R f' \sim_R f'',$$
  denn die Vertauschungen zweier Komponenten und das Addieren der i-ten Komponente mit $r \cdot f_j$ erfolgen durch Elementarmatrizen, welche invertierbar sind.

- Sei f unimodular. f lässt sich zu einer R-Basis ergänzen genau dann wenn,

  $$f \sim_R e_1 = (1, 0, \dots, 0) \in R^n$$

  Dies folgt aus der Tatsache, dass $e_1 \cdot A = f$ mit $A \in \mathrm{GL}_n(R)$ und A als erste Spalte f hat.

- Sei $n = 2$, dann lässt sich jeder unimodulare Vektor $f = (f_1, f_2)$ zu einer Basis ergänzen. Denn es gibt $r_1, r_2 \in R$, sodass $r_1 \cdot f_1 + r_2 \cdot f_2 = 1$ und für

  $$A := \begin{pmatrix} r_1 & -f_2 \\ r_2 & f_1 \end{pmatrix} \text{ gilt } (f_1, f_2) \cdot A = (r_1 \cdot f_1 + r_2 \cdot f_2, -f_1 \cdot f_2 + f_2 \cdot f_1) = (1, 0).$$

  A ist invertierbar, denn $\det(A) = r_1 \cdot f_1 + r_2 \cdot f_2 = 1$.

Konvention
Seien $f, g \in R^n$, $I \subseteq R$ ein Ideal, $\pi : R \to R/I$ die kanonische Projektion, $S \subseteq R$ eine multiplikativ abgeschlossene Teilmenge und $\varphi : R \to RS^{-1}$ der kanonische Ringhomomorphismus. Des Weiteren seien

$$\pi_n : R^n \to (R/I)^n, (f_1, \ldots, f_n) \mapsto (\pi(f_1), \ldots, \pi(f_n))$$

und

$$\varphi_n : R^n \to (RS^{-1})^n, (f_1, \ldots, f_n) \mapsto (\varphi(f_1), \ldots, \varphi(f_n))).$$

Falls $\pi_n(f) \sim_{R/I} \pi_n(g)$ bzw. $\varphi_n(f) \sim_{RS^{-1}} \varphi_n(g)$, so werden wir im restlichen Verlauf dieser Bachelorarbeit stets $f \sim_{R/I} g$ bzw. $f \sim_{RS^{-1}} g$ verwenden.

Notation
Sei $I \subseteq R[t]$ ein Ideal und $m \in \mathbb{N}$. Wir setzen

$$\mathrm{H}_m(I) := \operatorname{span}_R(\{r \in R \mid \exists r_0, \ldots, r_{m-1} \in R \quad r \cdot t^m + \sum_{i=0}^{m-1} r_i \cdot t^i \in I\}).$$

Mit anderen Worten, $\mathrm{H}_m(I)$ ist ein Ideal, welches aus den Höchstkoeffizienten von $g \in I$ mit $\deg(g) = m$ besteht.

Lemma von Suslin 3.5
Sei $I \subseteq R[t]$ ein Ideal mit $f \in I$, wobei f normiert ist mit $\deg(f) = m + 1 \in \mathbb{N}$. Für $g \in I$ mit $\deg(g) \leq m$ liegen alle Koeffizienten von g in $\mathrm{H}_m(I)$.

Beweis (vgl. [La06] Lemma III.2.8)
Seien $g = \sum_{i=0}^{m} a_i \cdot t^{m-i}$ und $f = \sum_{i=0}^{m+1} b_i \cdot t^{m+1-i}$ mit $a_i, b_i \in R$ und $b_0 \in R^\times$. Wir zeigen die Aussage per Induktion über die Koeffizientenindizes. Der Induktionsanfang ist per Definition von $\mathrm{H}_m(I)$ klar. Nun nehmen wir an, dass die Aussage für ein festes n gilt und betrachten

$$\begin{aligned} t \cdot g - a_0 \cdot b_0^{-1} \cdot f &= \sum_{i=0}^{m} a_i \cdot t^{m+1-i} - a_0 \cdot b_0^{-1} \cdot \sum_{i=0}^{m+1} b_i \cdot t^{m+1-i} \\ &= -a_0 \cdot b_0^{-1} \cdot b_{m+1} + \sum_{i=1}^{m} (a_i - a_0 \cdot b_0^{-1} \cdot b_i) \cdot t^{m+1-i} \\ &= -a_0 \cdot b_0^{-1} \cdot b_{m+1} + \sum_{i=0}^{m-1} (a_{i+1} - a_0 \cdot b_0^{-1} \cdot b_{i+1}) \cdot t^{m-i} \\ &= \sum_{i=0}^{m} c_i \cdot t^{m-i}, \end{aligned}$$

wobei $c_m = -a_0 \cdot b_0^{-1} \cdot b_{m+1}$ und $c_i = a_{i+1} - a_0 \cdot b_0^{-1} \cdot b_{i+1}$ für alle $i \in \underline{m-1}$.
Nach Induktionsbehauptung gilt nun, dass $c_1, \ldots, c_n \in \mathrm{H}_m(I)$. Nach einer Umformung erhalten wir aus

$$c_n = a_{n+1} - a_0 \cdot b_0^{-1} \cdot b_{i+1} \text{ die Gleichung } a_{n+1} = c_n - a_0 \cdot b_0^{-1} \cdot b_{i+1}.$$

Da $c_n, a_0 \in \mathrm{H}_m(I)$ und $\mathrm{H}_m(I)$ ein Ideal ist, ist auch $a_{n+1} \in \mathrm{H}_m(I)$. □

Satz von Horrocks 3.6
Sei R ein lokaler Ring mit dem maximalem Ideal $\mathfrak{m}$ und $f = (f_1, \dots, f_n) \in R[t]^n$ ein unimodularer Vektor, wobei es $i \in \underline{n}$ gibt, sodass f_i normiert ist.
Dann lässt sich f zu einer Basis von $R[t]^n$ ergänzen.

Beweis (vgl. [La06] alternativer Beweis zu III.2.6 im Abschnitt unter Lemma III.2.8)
Sei $f \in R[t]^n$ wie oben. Für $n = 1$ ist f_1 eine Einheit und bildet somit eine $R[t]$-Basis von $R[t]$. Bei $n = 2$ sei ohne Einschränkung f_1 normiert, dann ist $((f_1, f_2), (0, 1))$ eine $R[t]$-Basis von $R[t]^2$. Sei nun $n \geq 3$ und wir setzen d als das Minimum der Grade von f_i, die normiert sind und zeigen nun per Induktion, dass sich f für alle d zu einer $R[t]$-Basis von $R[t]^n$ ergänzen lässt. Für $d = 0$ wäre ein f_i eine Einheit und somit lässt sich f durch die Einheitsvektoren e_j mit $i \neq j$ zu einer Basis ergänzen. Wir nehmen nun an, dass die Aussage für ein festes $d \in \mathbb{N}$ gelte, d.h. besitzt ein unimodularer Vektor ein normiertes Polynom mit Grad $\leq d$, so lässt sich dieser zu einer Basis ergänzen. Sei jetzt f ein unimodularer Vektor, wobei der kleinste Grad des normierten Polynomes gleich $d + 1$ ist. Wir nehmen ohne Einschränkung an, dass f_1 normiert ist und Grad $d+1$ besitzt. Wir wenden nun für alle $i \in \underline{n}\backslash\{1\}$ die Division mit Rest auf f_j und f_1 an. Dies ist hier möglich, da f_1 normiert ist. Somit erhalten wir

$$f_i = q_i \cdot f_1 + f_i' \text{ mit } \deg(f_i') < \deg(f_1) = d + 1$$

und setzen nun

$$f' := (f_1, f_2', \dots, f_n').$$

Falls für ein $i \in \underline{n}\backslash\{1\}$ f_i' normiert ist, so können wir die Induktionsvoraussetzung auf f' anwenden und sind fertig, denn $f \sim_{R[t]} f'$. Daher nehmen wir nun an, dass f_i' nicht normiert ist. f' ist unimodular, denn es gibt $g_1, \dots, g_n \in R[t]$, sodass

$$\begin{aligned} 1 &= \sum_{i=1}^{n} g_i \cdot f_i = g_1 \cdot f_1 + \sum_{i=2}^{n} g_i \cdot (q_i \cdot f_1 + f_i') \\ &= f_1 \cdot (g_1 + \sum_{i=2}^{n} g_i \cdot q_i \cdot f_i) + \sum_{i=2}^{n} g_i \cdot f_i'. \end{aligned}$$

Aus obiger Gleichung entnimmt man auch, dass $f' \mod \mathfrak{m}$ ein unimodularer Vektor ist. Daher besitzt eines der Polynome $f_2', \dots, f_n'$ mindestens einen Koeffizienten $c \notin \mathfrak{m}$. Anderenfalls würde aus $1 = f_1 \cdot (g_1 + \sum_{i=2}^{n} g_i \cdot q_i \cdot f_i) + 0 \mod \mathfrak{m}$ folgen, dass $f_1 \mod \mathfrak{m}$ eine Einheit in $(R/\mathfrak{m})[t]$ ist, aber $\deg(f_1 \mod \mathfrak{m}) = \deg(f_1) = d + 1 \geq 1$. Wir nehmen ohne Einschränkung an, dass f_2' einen solchen Koeffizienten c besitzt und wenden nun Lemma 3.5 auf $I := \mathrm{span}_{R[t]}(f_1, f_2')$ an. Daher existiert ein Polynom

$$h := h_1 \cdot f_1 + h_2 \cdot f_2' \in I$$

vom Grad d mit Höchstkoeffizient c. Sei nun

$$f_3'' := f_3' + h \text{ und somit } f \sim_{R[t]} f' \sim_{R[t]} (f_1, f_2', f_3'', f_4', \ldots, f_n') =: f''.$$

f_3' ist nicht normiert und daher liegt dessen Höchstkoeffizient in $\mathfrak{m}$. Wegen $\deg(h) = d \geq \deg(f_3')$, liegt der Höchstkoeffizient von f_3'' in $c + \mathfrak{m}$ und ist daher eine Einheit. Nun besitzt f_3'' Grad d und wir können daher die Induktionsvoraussetzung anwenden. Nun lässt sich f'' zu einer $R[t]$-Basis von R^n ergänzen und somit auch f. □

Korollar 3.7
Seien R und f wie im obigen Satz. Dann gilt $f(t) \sim_{R[t]} f(0)$.

Beweis (vgl. [La02] Korollar XXI.3.2)
$f(t)$ lässt sich zu einer $R[t]$-Basis von $R[t]^n$ ergänzen und daher ist $f(t) \sim_{R[t]} e_1$, wobei e_1 der erste Einheitsvektor ist. Also finden wir eine geeignete Matrix $A(t) \in \mathrm{GL}_n(R[t])$, sodass $f(t) \cdot A(t) = e_1$. Nun gilt für $t = 0$, aber $f(0) \cdot A(0) = e_1$ und somit $f(0) \sim_{R[t]} e_1$. Daher erhalten wir $f(t) \sim_{R[t]} f(0)$. □

Lemma 3.8
Sei $S \subseteq R$ multiplikativ abgeschlossen und $\varphi : R \to RS^{-1}$ der kanonische Ringhomomorphismus. Wir definieren den Ringhomomorphismus $\varphi_t : R[t] \to RS^{-1}[t]$ als

$$\varphi_t(\sum_{i=0}^{m} a_i \cdot t^i) = \sum_{i=0}^{m} \varphi(a_i) \cdot t^i = \sum_{i=0}^{m} \frac{a_i}{1} \cdot t^i.$$

Ferner sei $A(t) := (a_{ij}(t))_{i,j\in\underline{n}} \in \mathrm{GL}_n(RS^{-1}[t])$ mit $A(0) = \mathrm{I}_n$. Dann gibt es eine Matrix $B(t) := (b_{ij}(t))_{i,j\in\underline{n}} \in \mathrm{GL}_n(R[t])$ mit $B(0) = \mathrm{I}_n$ und ein $s \in S$, sodass $B(t)$ zu $A(st)$ lokalisiert wird, d.h. für alle $i, j \in \underline{n}$ gilt $\varphi_t(b_{ij}(t)) = a_{ij}(st)$.

Beweis (vgl. [La06] Lemma III.2.2)
Sei $A(t)$ wie oben. $A(0) = \mathrm{I}_n$ impliziert, dass die Einträge von $A(t)$ die Gestalt

$$a_{ij}(t) \in t \cdot RS^{-1}[t] \text{ und } a_{ii}(t) \in 1 + t \cdot RS^{-1}[t],$$

für alle $i, j \in \underline{n}$ mit $i \neq j$, besitzen. Dies gilt auch für die Einträge von $A(t)^{-1}$, denn die Auswertung bei $t = 0$ ergibt $A(0)^{-1} = \mathrm{I}_n^{-1} = \mathrm{I}_n$. Für $i, j \in \underline{n}$ haben wir daher

$$a_{ij}(t) = \sum_{k=0}^{m_{ij}} \frac{r_{ij}^{(k)}}{s_{ij}^{(k)}} \cdot t^k + \delta_{ij} \text{ mit } r_{ij}^{(k)} \in R,\ s_{ij}^{(k)} \in S \text{ und } \delta_{ij} = \begin{cases} 0 & i \neq j \\ 1 & i = j. \end{cases}$$

Wir setzen nun

$$s_A := \prod_{i,j\in\underline{n}} \prod_{k=0}^{m_{ij}} s_{ij}^{(k)} \in S$$

und $s := s_A \cdot s_{A^{-1}}$, wobei $s_{A^{-1}}$ ähnlich konstruiert wurde. Sei jetzt $B(t) = (b_{ij}(t))_{i,j\in\underline{n}}$ mit $b_{ij}(t) \in R[t]$ und $B(0) = \mathrm{I}_n$, sodass

$$\varphi_t(b_{ij}(t)) = \sum_{k=0}^{m_{ij}} \frac{r_{ij}^{(k)}}{s_{ij}^{(k)}} \cdot s^k \cdot t^k + \delta_{ij}$$

Für $A^{-1} := (a'_{ij}(t))_{i,j\in\underline{n}}$ konstruieren wir auf ähnliche Weise eine Matrix $C(t) := (c_{ij}(t))_{i,j\in\underline{n}}$ mit $C(0) = \mathrm{I}_n$ und $\varphi_t(c_{ij}(t)) = a'_{ij}(st)$. Dann gilt $\varphi_t(b_{ij}(t)) = a_{ij}(st)$. Es verbleibt noch zu zeigen, dass $B(t)$ invertierbar ist. Sei $D(t) := (d_{ij}(t))_{i,j\in\underline{n}}$ das Produkt der beiden Matrizen $B(t)$ und $C(t)$. Nun gilt aber für jeden Eintrag von $D(t)$, dass

$$\begin{aligned}
\frac{d_{ij}(t)}{1} &= \varphi_t(d_{ij}(t)) \\
&= \varphi_t(\sum_{k=0}^{n} b_{ik}(t) \cdot c_{kj}(t)) \\
&= \sum_{k=0}^{n} \varphi_t(b_{ik}(t)) \cdot \varphi_t(c_{kj}(t)) \\
&= \sum_{k=0}^{n} a_{ik}(st) \cdot a'_{kj}(st) = \delta_{ij}.
\end{aligned}$$

Dies zeigt, dass alle Koeffizienten aller $d_{ij}(t)$ mit $i \neq j$ S-Torsionselemente sind, d.h. von geeigneten Elementen in S annulliert werden. Wie oben konstruiert man $s' \in S$ mit $\mathrm{I}_n = D(s't) = B(s't) \cdot C(s't)$ über $R[t]$. Indem man $B(t)$ durch $B(s't)$ ersetzt, ist also $B(t)$ wie gewünscht.

□

Proposition 3.9
Sei $S \subseteq R$ multiplikativ abgeschlossen und $f \in R[t]^n$ unimodular. Ferner bezeichnen wir mit x eine weitere Variable. Dann sind äquivalent:

(i) $f(t) \sim_{RS^{-1}[t]} f(0)$.

(ii) Es gibt ein $s \in S$, sodass $f(t + sx) \sim_{R[t,x]} f(t)$.

Beweis (vgl. [La06] Proposition III.2.3)
Für die Hinlänglichkeit sei $A(t) \in \mathrm{GL}_n(RS^{-1}[t])$, sodass $f(t) \cdot A(t) = f(0)$ und setze $B(t, x) := A(t + x) \cdot A(t)^{-1} \in \mathrm{GL}_n(RS^{-1}[t, x])$. Dann gilt

$$\begin{aligned}
f(t + x) \cdot B(t, x) &= f(t + x) \cdot A(t + x) \cdot A(t)^{-1} \\
&= f(0) \cdot A(t)^{-1} \\
&= f(t)
\end{aligned}$$

und somit $f(t+x) \sim_{RS^{-1}[t,x]} f(t)$. Wegen $B(t, 0) = A(t) \cdot A(t)^{-1} = \mathrm{I}_n$ können wir Lemma 3.8 anwenden. Dadurch finden wir nun ein $C(t, x) \in \mathrm{GL}_n(R[t, x])$ und ein $s \in S$, sodass $C(t,0) = \mathrm{I}_n$ und $C(t,x)$ zu $B(t,sx)$ lokalisiert wird. Wegen $f(t) = f(t + s \cdot 0) \cdot C(t,0)$ folgt, dass es $g(t,x) \in R[t]^n$ gibt mit

$$f(t+sx) \cdot C(t,x) - f(t) = x \cdot g(t,x)$$

und sodass $g(t,x)$ nach Lokalisieren 0 wird. Es gibt also $s' \in S$ mit $s' \cdot g(t,x) = 0$ und daher

$$f(t+ss'x) \cdot C(t,s'x) = f(t) \text{ mit } C(t,s'x) \in \mathrm{GL}_n(R[t,x]).$$

Für die Rückrichtung betrachte den Ringhomomorphismus $R[t,x] \to RS^{-1}[t], t \mapsto 0$ und $x \mapsto s^{-1}t$. Wir erhalten dann

$$f(0 + s \cdot s^{-1} \cdot t) = f(t) \sim_{RS^{-1}[t]} f(0).$$

□

Proposition 3.10
Sei R ein Ring und $f = (f_1, \dots, f_n) \in R[t]^n$ unimodular. Wir setzen $\mathfrak{a} := \{a \in R \mid f(t) \sim_{R_a[t]} f(0)\}$, wobei $R_a := RS^{-1}$ mit $S = \{a^n \mid n \in \mathbb{N}\}$ und $\mathfrak{b} = \{b \in R \mid f(t+bx) \sim_{R[t,x]} f(t)\}$. Die Mengen $\mathfrak{a}$ und $\mathfrak{b}$ sind Ideale und es gilt $\mathfrak{a} = \mathrm{Rad}(\mathfrak{b}) = \{r \in R \mid \exists\, n \in \mathbb{N}\ r^n \in b\}$.

Beweis (vgl. [La06] Theorem III.2.4)
Wir zeigen zuerst, dass $\mathfrak{b}$ ein Ideal ist. Hierbei ist $0 \in \mathfrak{b}$ klar und für $b_1, b_2 \in \mathfrak{b}$ ersetzen wir t durch $t + b_1 x$ und erhalten

$$f(t + b_1 + b_2) \underset{R[t,x]}{\sim} f(t + b_2 x) \underset{R[t,x]}{\sim} f(t)$$

und somit $b_1 + b_2 \in \mathfrak{b}$. Für die Abgeschlossenheit ersetzen wir $r \in R$ und x durch rx und für ein beliebiges $b \in \mathfrak{b}$ gilt dann

$$f(t) \underset{R[t,x]}{\sim} f(t+bx) \underset{R[t,x]}{\sim} f(t+brx).$$

Nun zeigen wir, dass $\mathfrak{a} = \mathrm{Rad}(\mathfrak{b})$, womit auch gezeigt wäre, dass $\mathfrak{a}$ ein Ideal ist. Für $a \in \mathfrak{a}$, d.h. $f(t) \sim_{R_a[t]} f(0)$ gibt es nach Proposition 3.9 ein $s \in \{1, a, \dots, \}$, sodass

$$f(t+sx) \underset{R[t,x]}{\sim} f(t).$$

Dies zeigt, dass $a \in \mathrm{Rad}(\mathfrak{b})$. Sei $b \in \mathrm{Rad}(\mathfrak{b})$, dann gibt es ein $n \in \mathbb{N}$, sodass $b^n \in \mathfrak{b}$. Für b^n gilt auch nach der voherigen Proposition 3.9 $f(t) \sim_{R_b[t]} f(0)$ und somit $b \in \mathfrak{a}$. □

Satz 3.11
Sei $f = (f_1, \dots, f_n) \in R[t]^n$ unimodular.

(i) Für alle maximalen Ideale $\mathfrak{m} \subseteq R$ gelte $f(t) \sim_{R_\mathfrak{m}[t]} f(0)$. Dann gilt auch $f(t) \sim_{R[t]} f(0)$.

(ii) Es gebe ein $i \in \underline{n}$, sodass f_i normiert ist. Dann gilt bereits $f(t) \sim_R f(0)$.

Beweis (vgl. [La06] Theorem III.2.5)

(i) Seien $\mathfrak{a}$ und $\mathfrak{b}$ die Ideale wie in der vorherigen Proposition. Angenommen $\mathfrak{b} \neq R$, dann gibt es für $\mathfrak{b}$ ein maximales Ideal $\mathfrak{m}$, sodass $\mathfrak{b} \subseteq \mathfrak{m}$. Jedoch gilt nach Voraussetzung, dass $f(t) \sim_{R_\mathfrak{m}[t]} f(0)$ und nach den beiden letzten Propositionen gibt es ein $r \in R \backslash \mathfrak{m}$, sodass $f(t+rx) \sim_{R[t,x]} f(t)$, womit $r \in \mathfrak{b} \subseteq \mathfrak{m}$, was ein Widerspruch bildet. Daraus folgt nun, dass $\mathfrak{b}$ das Einsideal bildet. Aus $\mathfrak{a} = \operatorname{Rad}(\mathfrak{b}) = R$ folgt somit die Aussage.

(ii) Dies folgt aus (i) und Korollar 3.7.

□

Lemma 3.12
Seien $\mathfrak{p}_1, \ldots, \mathfrak{p}_n \in \operatorname{Spec}(R)$, $r \in R$ und $I \subseteq R$ ein Ideal. Falls $r + I \subseteq \bigcup_{i=1}^n \mathfrak{p}_i$, so ist $\operatorname{span}_R(r, I) \subseteq \mathfrak{p}_i$ für ein $i \in \underline{n}$.

Beweis (vgl. [La06] Lemma II.7.4)
Angenommen die Aussage sei für n falsch, wobei n minimal gewählt ist, d.h. ist $r + I \subseteq \bigcup_{i=1}^m \mathfrak{q}_i$ mit $m > n$ und Primidealen $\mathfrak{q}_1, \ldots, \mathfrak{q}_m$, so ist $\operatorname{span}_R(r, I) \subseteq \mathfrak{q}_i$ für ein $i \in \underline{m}$. Aus unserer Annahme und der Minimalität von n erhalten wir, dass $n > 1$ und $\mathfrak{p}_i \not\subseteq \mathfrak{p}_j$ für $i \neq j$. Wir zeigen nun per Widerspruch, dass $r \in \bigcap_{i=1}^n \mathfrak{p}_i$. Wäre $r \notin \mathfrak{p}_i$ für ein $i \in \underline{n}$, so wäre

$$(r + \mathfrak{p}_i \cdot I) \cap \mathfrak{p}_i = \{0\} \text{ und folglich } x + \mathfrak{p}_\mathrm{i} \cdot I \subseteq \bigcup_{\substack{j=1 \\ j \neq i}}^n \mathfrak{p}_j.$$

Aufgrund der Minimalität von n, haben wir $\operatorname{span}_R(r, \mathfrak{p}_i \cdot I) \subseteq \mathfrak{p}_j$ für ein $j \neq i$. Wegen $\mathfrak{p}_i \not\subseteq \mathfrak{p}_j$ existiert $y \in \mathfrak{p}_i \backslash \mathfrak{p}_j$. Dann ist für jedes $z \in I$ aber $y \cdot z \in \mathfrak{p}_i \cdot I \subseteq \mathfrak{p}_j$ und daher $z \in \mathfrak{p}_j$, da $\mathfrak{p}_j$ prim ist. Es folgt $I \subseteq \mathfrak{p}_j$ und daher $\operatorname{span}_R(r, I) \subseteq \mathfrak{p}_j$. Dies steht im Widerspruch zu unserer ersten Annahme, daher ist $r \in \bigcap_{i=1}^n \mathfrak{p}_i$. Jetzt können wir daraus und aus $r + I \subseteq \bigcup_{i=1}^n \mathfrak{p}_i$ folgern, dass bereits $I \subseteq \bigcup_{i=1}^n \mathfrak{p}_i$. Wieder aufgrund der Minimalität von n, ist

$$I \not\subseteq \bigcup_{\substack{j=1 \\ j \neq i}}^n \mathfrak{p}_i =: J_i,$$

für alle $i \in \underline{n}$. Sei nun $s_i \in I \backslash J_i$. Da $I \subseteq J_i \cup \mathfrak{p}_i$ ist auch $s_i \in \mathfrak{p}_i$. Nun ist

$$s := \sum_{i=1}^n \prod_{\substack{j=1 \\ j \neq i}}^n s_j \in I,$$

aber für alle $i \in \underline{n}$, ist $s \notin \mathfrak{p}_i$, denn sonst gäbe es $i \in \underline{n}$ mit

$$s_1 \cdot \ldots \cdot s_{i-1} \cdot s_{i+1} \cdot \ldots \cdot s_n = s - s_i \cdot \sum_{\substack{k=1 \\ k \neq i}}^n \prod_{\substack{j=1 \\ j \neq k,i}}^n s_j \in \mathfrak{p}_i$$

und dementsprechend $s_j \in \mathfrak{p}_i$, für ein $j \neq i$, da $\mathfrak{p}_i$ ein Primideal ist. Wegen

$$\mathfrak{p}_i \subseteq \bigcup_{\substack{k=1 \\ k \neq j}}^{n} \mathfrak{p}_k = J_j$$

steht das im Widerspruch zu $s_j \notin J_j$. Daher ist $s \notin \bigcup_{i=1}^{n} \mathfrak{p}_\mathfrak{i}$, was einen Widerspruch bildet. $\square$

Lemma 3.13
Sei R ein noetherscher Ring und $(r_1, \ldots, r_n) \in R^n$ ein unimodularer Vektor. Dann gibt es ein $(s_1, \ldots, s_n) \in R^n$, sodass $(r_1, \ldots, r_n) \sim_R (s_1, \ldots, s_n)$ und für alle $m \leq n$ gilt $\mathrm{ht}(\mathrm{span}_R(s_1, \ldots, s_m)) \geq m$.

Beweis (vgl. [La06] Lemma III.3.4)
Wir gehen schrittweise vor. Für $m = 1$ und r_1 nicht nilpotent haben wir bereits $\mathrm{ht}(\mathrm{span}_R(r_1)) \geq 1$, da das Nilradikal von R der Durchschnitt aller minimalen Primideale ist. Falls r_1 nilpotent ist, so vertauschen wir r_1 mit einem nicht nilpotenten r_i, für $i \in \{2, \ldots, n\}$. Solch ein r_i existiert, da $(r_1, \ldots, r_n)$ unimodular ist und somit nicht alle Einträge nilpotent sein können. Nun nehmen wir an, dass bereits $\mathrm{ht}(I) \geq m$ gilt mit $m \leq n$ und $I := \mathrm{span}_R(r_1, \ldots, r_m)$. Wir bezeichnen mit $\bar{r}$ das Bild der kanonischen Projektion von $r \in R$ in R/I. Da $(r_1, \ldots, r_n)$ unimodular ist, gibt es $a_1, \ldots, a_n \in R$ mit

$$\bar{1} = \sum_{i=1}^{n} \bar{a}_i \cdot \bar{r}_i = \sum_{i=m+1}^{n} \bar{a}_i \cdot \bar{r}_i, \text{ da } \bar{r}_1 = \ldots = \bar{r}_m = 0_{R/I}.$$

Dies zeigt, dass $(\bar{r}_{m+1}, \ldots, \bar{r}_n)$ ein unimodularer Vektor in $(R/I)^{n-m-1}$ ist. Da auch R/I noethersch ist und besitzt R/I nur endlich viele minimale Primideale $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$. Sei nun $J := \mathrm{span}_{R/I}(\bar{r}_{m+2}, \ldots, \bar{r}_n)$. Nun ist $\mathrm{span}_{R[t]}(\bar{r}_{m+1}, J) = (R/I)[t] \not\subseteq \mathfrak{q}_i$ für alle $i \in \underline{r}$ und aus der Kontrapositon von Lemma 3.12 folgt dann, dass $\bar{r}_{m+1} + J \not\subseteq \bigcup_{i=1}^{r} \mathfrak{q}_i$. Daher existieren $\bar{b}_{m+2}, \ldots, \bar{b}_n \in R/I$ derart, dass

$$\bar{r}'_{m+1} := \bar{r}_{m+1} + \bar{b}_{m+2} \cdot \bar{r}_{m+2} + \ldots + \bar{b}_n \cdot \bar{r}_n \notin \bigcup_{i=1}^{r} \mathfrak{q}_i.$$

Nun ersetzen wir r_i durch $r'_i = r_{m+1} + b_{m+2} \cdot r_{m+2} + \ldots + b_n \cdot r_n \in R$. Dann gilt

$$(r_1, \ldots, r'_i, \ldots, r_n) \sim_R (r_1, \ldots, r_i, \ldots, r_n).$$

Sei $\mathfrak{p}$ ein Primideal mit $\mathrm{span}_R(r_1, \ldots, r_m, r'_{m+1}) \subseteq \mathfrak{p}$. Da $\bar{r}'_{m+1} \in \bar{\mathfrak{p}}$, kann $\bar{\mathfrak{p}} \subseteq R/I$ nicht minimal sein. Daher gibt es ein minimales Primideal $\mathfrak{q}_i$ mit $\mathfrak{q}_i \subsetneq \bar{\mathfrak{p}}$. Das Urbild $\mathfrak{p}_i$ von $\mathfrak{q}_i$ unter $R \to R/I$ ist wieder ein Primideal und aus $I \subseteq \mathfrak{p}_i \subsetneq \mathfrak{p}$ folgt, dass

$$\mathrm{ht}(\mathfrak{p}) > \mathrm{ht}(\mathfrak{p}_i) \geq \mathrm{ht}(I) \geq m.$$

Somit haben wir $\mathrm{ht}(\mathfrak{p}) \geq m + 1$, was wiederum $\mathrm{ht}(\mathrm{span}_R(r_1, \ldots, r'_{m+1})) \geq m + 1$ impliziert, da $\mathfrak{p}$ beliebig war. $\square$

Satz 3.14
Sei R ein Hauptidealring. Dann besitzt $R[t_1, \ldots, t_n]$ die unimodulare Erweiterungseigenschaft.

Beweis (vgl. [La06] Theorem III.3.5)
Wir beweisen auch dies per Induktion über die Anzahl der Variablen.
Für $n = 0$ ist R ein Hauptidealring und für einen unimodularen Vektor $f = (f_1, \ldots, f_m) \in R^m$ ist der Modul $R^m/\operatorname{span}_R(f)$ torsionsfrei und daher frei. Wir wählen dann $g_1, \ldots, g_{m-1} \in R^m$, deren Bilder in $R^m/\operatorname{span}_R(f)$ eine Basis bilden. Dann ist $(f, g_1, \ldots, g_{m-1})$ eine Basis von R^m. Sei $n \in \mathbb{N}\backslash\{0\}$ beliebig und $R[t_1, \ldots, t_n]$ besitze die unimodulare Erweiterungsschaft. Wir zeigen nun, dass auch $R[t_1, \ldots, t_{n+1}]$ diese besitzt. Sei dazu $f \in R[t_1, \ldots, t_{n+1}]^m$ ein unimodularer Vektor und $m \in \mathbb{N}$. Für $m = 1$ ist f eine Einheit und bildet somit eine Basis. Den Fall $m = 2$ haben wir in einer Bemerkung unter Definition 3.4 behandelt. Sei daher also $m \geq 3$. Nach Lemma 3.13 finden wir ein $g \in R[t_1, \ldots, t_{n+1}]^m$ mit $f \sim_{R[t_1,\ldots,t_{n+1}]} g$ derart, dass

$$\operatorname{ht}(\operatorname{span}_{R[t_1,\ldots,t_{n+1}]}(g_1, \ldots, g_r)) \geq r \text{ für alle } r \leq m.$$

Setze nun $I := \operatorname{span}_{R[t_1,\ldots,t_{n+1}]}(g_1, \ldots, g_{m-1})$. Da $\operatorname{ht}(I) \geq m - 1 \geq 2 > \dim(R) \geq 1$ finden wir nach Satz 1.13, Variablen $s_1, \ldots, s_{n+1} \in R[t_1, \ldots, t_{n+1}]$, sodass $R[t_1, \ldots, t_{n+1}] = R[s_1, \ldots, s_{n+1}]$. Außerdem enthält I nun ein in s_{n+1} normiertes Polynom

$$h := g_1 \cdot h_1 + \ldots + g_{m-1} \cdot h_{m-1} \text{ mit } h_1, \ldots, h_{m-1} \in R[s_1, \ldots, s_{n+1}].$$

Nun setze $g'_m := g_m + s_{n+1}^k \cdot h$, wobei $k \in \mathbb{N}$ so gewählt ist, sodass $k \cdot \deg_{s_{n+1}}(h) > \deg_{s_{n+1}}(g_m)$. Jetzt enthält g ein in s_{n+1} normiertes Polynom. Satz 3.11 induziert die folgende Relationskette:

$$\begin{aligned} f \underset{R[s_1,\ldots,s_{n+1}]}{\sim} g \underset{R[s_1,\ldots,s_{n+1}]}{\sim} & (g_1, \ldots, g'_n) \\ \underset{R[s_1,\ldots,s_{n+1}]}{\sim} & (g_1(s_1, s_2, \ldots, 0), \ldots, g'_n(s_1, s_2, \ldots, 0)) =: f' \end{aligned}$$

f' ist ein unimodularer Vektor in S^m mit $S = R[s_1, \ldots, s_n] \subseteq R[t_1, \ldots, t_{n+1}]$. Da S die unimodulare Erweiterungseigenschaft besitzt, gilt $f' \sim (1, 0, \ldots, 0)$ über S und damit über $R[t_1, \ldots, t_{n+1}]$. □

Nun sind wir in der Lage den Satz von Quillen-Suslin zu beweisen.

Satz von Quillen-Suslin
Sei R ein Hauptidealring. Dann ist jeder endlich erzeugte, projektive $R[t_1, \ldots, t_n]$-Modul frei.

Beweis
Nach Satz 2.13 ist jeder endlich erzeugte, projektive $R[t_1, \ldots, t_n]$-Modul stabil frei. $R[t_1, \ldots, t_n]$ besitzt nach Satz 3.14 die unimodulare Erweiterungseigenschaft. Jetzt besagt Satz 3.3, dass jeder stabil freie $R[t_1, \ldots, t_n]$-Modul frei ist. □

Literatur

[Bo13] Bosch, Siegfried: Algebraic Geometry and Commutative Algebra, Springer Verlag, 2013

[La02] Lang, Serge: Algebra (3rd Edition), Springer Verlag, 2002

[La06] Lam, Tsit Yuen: Serre's Problem on Projective Modules, Springer Verlag, 2006

[Ro94] Rosenberg, Jonathan: Algebraic K-Theory and Its Applications, Springer-Verlag, 1994

Eidesstattliche Versicherung

Ich erkläre hiermit an Eides Statt, dass ich die vorliegende Bachelorarbeit selbstständig und ohne Benutzung anderer, als der angegebenen Hilfsmittel, angefertigt habe. Die aus anderen Quellen direkt oder indirekt übernommenen Gedanken sind als solche gekennzeichnet.
Diese Arbeit wurde bisher in gleicher oder ähnlicher Form keiner anderen Prüfungsbehörde vorgelegt und auch noch nicht veröffentlicht.

Essen, den

Yogendra Puvanenthiran