§2.6 Minimale und reduzierte Gröbnerbasen

Generalvoraussetzung

In diesem Abschnitt sei stets K ein Körper.

Ferner sei eine Monomordnung $\leq$ auf $[X]$ fixiert.

Lemma. Sei $M \subseteq [\underline{X}]$ und $I := (M)$.

Lemma. Sei $M \subseteq [\underline{X}]$ und $I := (M)$. Dann ist die Menge

$$M' := \{v \in M \mid \nexists u \in M : (u \neq v \ \& \ u|v)\}$$

Lemma. Sei $M \subseteq [\underline{X}]$ und $I := (M)$. Dann ist die Menge

$$M' := \{v \in M \mid \nexists u \in M : (u \neq v \ \& \ u|v)\}$$

der bezüglich der Teilerrelation minimalen Elemente von M

Lemma. Sei $M \subseteq [\underline{X}]$ und $I := (M)$. Dann ist die Menge

$$M' := \{v \in M \mid \nexists u \in M : (u \neq v \ \& \ u|v)\}$$

der bezüglich der Teilerrelation minimalen Elemente von M das kleinste aus Monomen bestehende Erzeugendensystem von I,

Lemma. Sei $M \subseteq [\underline{X}]$ und $I := (M)$. Dann ist die Menge

$$M' := \{v \in M \mid \nexists u \in M : (u \neq v \ \& \ u|v)\}$$

der bezüglich der Teilerrelation minimalen Elemente von M das kleinste aus Monomen bestehende Erzeugendensystem von I, das heißt $I = (M')$ und für alle $M'' \subseteq [\underline{X}]$ mit $I = (M'')$ gilt $M' \subseteq M''$.

Lemma. Sei $M \subseteq [\underline{X}]$ und $I := (M)$. Dann ist die Menge

$$M' := \{v \in M \mid \nexists u \in M : (u \neq v \ \& \ u|v)\}$$

der bezüglich der Teilerrelation minimalen Elemente von M das kleinste aus Monomen bestehende Erzeugendensystem von I, das heißt $I = (M')$ und für alle $M'' \subseteq [\underline{X}]$ mit $I = (M'')$ gilt $M' \subseteq M''$. Insbesondere ist M' endlich.

Lemma. Sei $M \subseteq [\underline{X}]$ und $I := (M)$. Dann ist die Menge

$$M' := \{v \in M \mid \nexists u \in M : (u \neq v \ \& \ u|v)\}$$

der bezüglich der Teilerrelation minimalen Elemente von M das kleinste aus Monomen bestehende Erzeugendensystem von I, das heißt $I = (M')$ und für alle $M'' \subseteq [\underline{X}]$ mit $I = (M'')$ gilt $M' \subseteq M''$. Insbesondere ist M' endlich.

Beweis.
Zu zeigen:

(a) $M \subseteq (M')$

(b) $\forall M'' \subseteq [\underline{X}] : (I = (M'') \implies M' \subseteq M'')$

Lemma. Sei $M \subseteq [\underline{X}]$ und $I := (M)$. Dann ist die Menge

$$M' := \{v \in M \mid \nexists u \in M : (u \neq v \ \& \ u|v)\}$$

der bezüglich der Teilerrelation minimalen Elemente von M das kleinste aus Monomen bestehende Erzeugendensystem von I, das heißt $I = (M')$ und für alle $M'' \subseteq [\underline{X}]$ mit $I = (M'')$ gilt $M' \subseteq M''$. Insbesondere ist M' endlich.

Beweis.
Zu zeigen:

(a) $M \subseteq (M')$

(b) $\forall M'' \subseteq [\underline{X}] : (I = (M'') \implies M' \subseteq M'')$

Zu (a). Sei $w \in M$. Wähle $v \in M'$ mit $v|w$.

Lemma. Sei $M \subseteq [\underline{X}]$ und $I := (M)$. Dann ist die Menge

$$M' := \{v \in M \mid \nexists u \in M : (u \neq v \ \& \ u|v)\}$$

der bezüglich der Teilerrelation minimalen Elemente von M das kleinste aus Monomen bestehende Erzeugendensystem von I, das heißt $I = (M')$ und für alle $M'' \subseteq [\underline{X}]$ mit $I = (M'')$ gilt $M' \subseteq M''$. Insbesondere ist M' endlich.

Beweis.
Zu zeigen:

(a) $M \subseteq (M')$

(b) $\forall M'' \subseteq [\underline{X}] : (I = (M'') \implies M' \subseteq M'')$

Zu (a). Sei $w \in M$. Wähle $v \in M'$ mit $v|w$. Dann $w \in (M')$.

Lemma. Sei $M \subseteq [\underline{X}]$ und $I := (M)$. Dann ist die Menge

$$M' := \{v \in M \mid \nexists u \in M : (u \neq v \ \& \ u|v)\}$$

der bezüglich der Teilerrelation minimalen Elemente von M das kleinste aus Monomen bestehende Erzeugendensystem von I, das heißt $I = (M')$ und für alle $M'' \subseteq [\underline{X}]$ mit $I = (M'')$ gilt $M' \subseteq M''$. Insbesondere ist M' endlich.

Beweis.
Zu zeigen:

(a) $M \subseteq (M')$

(b) $\forall M'' \subseteq [\underline{X}] : (I = (M'') \implies M' \subseteq M'')$

Zu (a). Sei $w \in M$. Wähle $v \in M'$ mit $v|w$. Dann $w \in (M')$.

Zu (b). Sei $M'' \subseteq [\underline{X}]$ mit $I = (M'')$. Sei $v \in M'$. Zu zeigen ist $v \in M''$.

Lemma. Sei $M \subseteq [\underline{X}]$ und $I := (M)$. Dann ist die Menge

$$M' := \{v \in M \mid \nexists u \in M : (u \neq v \ \& \ u|v)\}$$

der bezüglich der Teilerrelation minimalen Elemente von M das kleinste aus Monomen bestehende Erzeugendensystem von I, das heißt $I = (M')$ und für alle $M'' \subseteq [\underline{X}]$ mit $I = (M'')$ gilt $M' \subseteq M''$. Insbesondere ist M' endlich.

Beweis.
Zu zeigen:

(a) $M \subseteq (M')$

(b) $\forall M'' \subseteq [\underline{X}] : (I = (M'') \implies M' \subseteq M'')$

Zu (a). Sei $w \in M$. Wähle $v \in M'$ mit $v|w$. Dann $w \in (M')$.

Zu (b). Sei $M'' \subseteq [\underline{X}]$ mit $I = (M'')$. Sei $v \in M'$. Zu zeigen ist $v \in M''$. Wegen $v \in M \subseteq I = (M'')$ gibt es $w \in M''$ mit $w|v$.

Lemma. Sei $M \subseteq [\underline{X}]$ und $I := (M)$. Dann ist die Menge

$$M' := \{v \in M \mid \nexists u \in M : (u \neq v \ \& \ u|v)\}$$

der bezüglich der Teilerrelation minimalen Elemente von M das kleinste aus Monomen bestehende Erzeugendensystem von I, das heißt $I = (M')$ und für alle $M'' \subseteq [\underline{X}]$ mit $I = (M'')$ gilt $M' \subseteq M''$. Insbesondere ist M' endlich.

Beweis.
Zu zeigen:

(a) $M \subseteq (M')$

(b) $\forall M'' \subseteq [\underline{X}] : (I = (M'') \implies M' \subseteq M'')$

Zu (a). Sei $w \in M$. Wähle $v \in M'$ mit $v|w$. Dann $w \in (M')$.

Zu (b). Sei $M'' \subseteq [\underline{X}]$ mit $I = (M'')$. Sei $v \in M'$. Zu zeigen ist $v \in M''$. Wegen $v \in M \subseteq I = (M'')$ gibt es $w \in M''$ mit $w|v$. Wegen $M'' \subseteq I = (M)$ gibt es $u \in M$ mit $u|w$.

Lemma. Sei $M \subseteq [\underline{X}]$ und $I := (M)$. Dann ist die Menge

$$M' := \{v \in M \mid \nexists u \in M : (u \neq v \ \& \ u|v)\}$$

der bezüglich der Teilerrelation minimalen Elemente von M das kleinste aus Monomen bestehende Erzeugendensystem von I, das heißt $I = (M')$ und für alle $M'' \subseteq [\underline{X}]$ mit $I = (M'')$ gilt $M' \subseteq M''$. Insbesondere ist M' endlich.

Beweis.
Zu zeigen:

(a) $M \subseteq (M')$

(b) $\forall M'' \subseteq [\underline{X}] : (I = (M'') \implies M' \subseteq M'')$

Zu (a). Sei $w \in M$. Wähle $v \in M'$ mit $v|w$. Dann $w \in (M')$.

Zu (b). Sei $M'' \subseteq [\underline{X}]$ mit $I = (M'')$. Sei $v \in M'$. Zu zeigen ist $v \in M''$. Wegen $v \in M \subseteq I = (M'')$ gibt es $w \in M''$ mit $w|v$. Wegen $M'' \subseteq I = (M)$ gibt es $u \in M$ mit $u|w$. Also $u|w|v$, woraus wegen $v \in M'$ und $u \in M$ folgt $u = w = v$, insbesondere $v = w \in M''$. $\square$

Lemma. Sei $I \subseteq K[\underline{X}]$ ein monomiales Ideal.

Lemma. Sei $I \subseteq K[\underline{X}]$ ein monomiales Ideal. Dann besitzt I genau ein aus Monomen bestehendes Erzeugendensystem M derart, dass kein Element von M ein anderes Element von M teilt.

Lemma. Sei $I \subseteq K[\underline{X}]$ ein monomiales Ideal. Dann besitzt I genau ein aus Monomen bestehendes Erzeugendensystem M derart, dass kein Element von M ein anderes Element von M teilt. Es ist M endlich und das kleinste aus Monomen bestehende Erzeugendensystem von I.

Lemma. Sei $I \subseteq K[\underline{X}]$ ein monomiales Ideal. Dann besitzt I genau ein aus Monomen bestehendes Erzeugendensystem M derart, dass kein Element von M ein anderes Element von M teilt. Es ist M endlich und das kleinste aus Monomen bestehende Erzeugendensystem von I. Man erhält M aus jedem anderen aus Monomen bestehenden Erzeugendensystem M' von I, indem man die bezüglich der Teilerrelation auf M' nicht minimalen Elemente aus M' entfernt.

Lemma. Sei $I \subseteq K[\underline{X}]$ ein monomiales Ideal. Dann besitzt I genau ein aus Monomen bestehendes Erzeugendensystem M derart, dass kein Element von M ein anderes Element von M teilt. Es ist M endlich und das kleinste aus Monomen bestehende Erzeugendensystem von I. Man erhält M aus jedem anderen aus Monomen bestehenden Erzeugendensystem M' von I, indem man die bezüglich der Teilerrelation auf M' nicht minimalen Elemente aus M' entfernt.

Beweis.
Um die Eindeutigkeit zu zeigen, sei $M \subseteq [\underline{X}]$ mit $I = (M)$ und $\forall u, v \in M : (u \neq v \implies u \nmid v)$.

Lemma. Sei $I \subseteq K[\underline{X}]$ ein monomiales Ideal. Dann besitzt I genau ein aus Monomen bestehendes Erzeugendensystem M derart, dass kein Element von M ein anderes Element von M teilt. Es ist M endlich und das kleinste aus Monomen bestehende Erzeugendensystem von I. Man erhält M aus jedem anderen aus Monomen bestehenden Erzeugendensystem M' von I, indem man die bezüglich der Teilerrelation auf M' nicht minimalen Elemente aus M' entfernt.

Beweis.
Um die Eindeutigkeit zu zeigen, sei $M \subseteq [\underline{X}]$ mit $I = (M)$ und $\forall u, v \in M : (u \neq v \implies u \not| v)$. Mit der Notation des letzten Lemmas gilt dann offenbar $M = M'$ und M' ist nach dem letzten Lemma durch I eindeutig bestimmt.

Lemma. Sei $I \subseteq K[\underline{X}]$ ein monomiales Ideal. Dann besitzt I genau ein aus Monomen bestehendes Erzeugendensystem M derart, dass kein Element von M ein anderes Element von M teilt. Es ist M endlich und das kleinste aus Monomen bestehende Erzeugendensystem von I. Man erhält M aus jedem anderen aus Monomen bestehenden Erzeugendensystem M' von I, indem man die bezüglich der Teilerrelation auf M' nicht minimalen Elemente aus M' entfernt.

Beweis.
Um die Eindeutigkeit zu zeigen, sei $M \subseteq [\underline{X}]$ mit $I = (M)$ und $\forall u, v \in M : (u \neq v \implies u \nmid v)$. Mit der Notation des letzten Lemmas gilt dann offenbar $M = M'$ und M' ist nach dem letzten Lemma durch I eindeutig bestimmt. Die Existenz und die restlichen Aussagen folgen ebenfalls aus dem letzten Lemma. $\square$

Minimale Gröbnerbasen

Definition. Eine Gröbnerbasis $G \subseteq K[\underline{X}]$ heißt minimal, wenn sie minimal unter allen Gröbnerbasen des von G erzeugten Ideals ist.

Minimale Gröbnerbasen

Definition. Eine Gröbnerbasis $G \subseteq K[\underline{X}]$ heißt minimal, wenn sie minimal unter allen Gröbnerbasen des von G erzeugten Ideals ist.

Proposition. Sei $G \subseteq K[\underline{X}] \setminus \{0\}$ endlich und $I := (G)$.
Dann sind äquivalent:

Minimale Gröbnerbasen

Definition. Eine Gröbnerbasis $G \subseteq K[\underline{X}]$ heißt minimal, wenn sie minimal unter allen Gröbnerbasen des von G erzeugten Ideals ist.

Proposition. Sei $G \subseteq K[\underline{X}] \setminus \{0\}$ endlich und $I := (G)$.
Dann sind äquivalent:

(a) G ist eine minimale Gröbnerbasis.

Minimale Gröbnerbasen

Definition. Eine Gröbnerbasis $G \subseteq K[\underline{X}]$ heißt minimal, wenn sie minimal unter allen Gröbnerbasen des von G erzeugten Ideals ist.

Proposition. Sei $G \subseteq K[\underline{X}] \setminus \{0\}$ endlich und $I := (G)$.
Dann sind äquivalent:

(a) G ist eine minimale Gröbnerbasis.

(b) G ist eine Gröbnerbasis derart, dass kein Leitmonom eines Elements von G das Leitmonom eines anderen Elements von G teilt.

Minimale Gröbnerbasen

Definition. Eine Gröbnerbasis $G \subseteq K[\underline{X}]$ heißt minimal, wenn sie minimal unter allen Gröbnerbasen des von G erzeugten Ideals ist.

Proposition. Sei $G \subseteq K[\underline{X}] \setminus \{0\}$ endlich und $I := (G)$.
Dann sind äquivalent:

(a) G ist eine minimale Gröbnerbasis.

(b) G ist eine Gröbnerbasis derart, dass kein Leitmonom eines Elements von G das Leitmonom eines anderen Elements von G teilt.

(c) Je zwei verschiedene Elemente von G haben verschiedene Leitmonome und

$$\{\mathrm{LM}(g) \mid g \in G\}$$

ist das kleinste aus Monomen bestehende Erzeugendensystem von $L(I)$.

Satz. Sei $I \subseteq K[\underline{X}]$ ein Ideal. Dann besitzt I eine minimale Gröbnerbasis.

Satz. Sei $I \subseteq K[\underline{X}]$ ein Ideal. Dann besitzt I eine minimale Gröbnerbasis. Sind G und H zwei minimale Gröbnerbasen von I, so gilt $\#G = \#H = \#\{\mathrm{LM}(g) \mid g \in G\}$

Satz. Sei $I \subseteq K[\underline{X}]$ ein Ideal. Dann besitzt I eine minimale Gröbnerbasis. Sind G und H zwei minimale Gröbnerbasen von I, so gilt $\#G = \#H = \#\{\mathrm{LM}(g) \mid g \in G\}$ und $\{\mathrm{LM}(g) \mid g \in G\} = \{\mathrm{LM}(h) \mid h \in H\}$.

Satz. Sei $I \subseteq K[X]$ ein Ideal. Dann besitzt I eine minimale Gröbnerbasis. Sind G und H zwei minimale Gröbnerbasen von I, so gilt $\#G = \#H = \#\{\mathrm{LM}(g) \mid g \in G\}$ und $\{\mathrm{LM}(g) \mid g \in G\} = \{\mathrm{LM}(h) \mid h \in H\}$.

Beweis.
Die zweite Aussage ist klar mit (c) aus der letzten Proposition.

Satz. Sei $I \subseteq K[\underline{X}]$ ein Ideal. Dann besitzt I eine minimale Gröbnerbasis. Sind G und H zwei minimale Gröbnerbasen von I, so gilt $\#G = \#H = \#\{\mathrm{LM}(g) \mid g \in G\}$ und $\{\mathrm{LM}(g) \mid g \in G\} = \{\mathrm{LM}(h) \mid h \in H\}$.

Beweis.
Die zweite Aussage ist klar mit (c) aus der letzten Proposition. Um die Existenz einer minimalen Gröbnerbasis von I zu zeigen, wähle man zunächst eine beliebige Gröbnerbasis $G \subseteq K[\underline{X}] \setminus \{0\}$ von I.

Satz. Sei $I \subseteq K[\underline{X}]$ ein Ideal. Dann besitzt I eine minimale Gröbnerbasis. Sind G und H zwei minimale Gröbnerbasen von I, so gilt $\#G = \#H = \#\{\mathrm{LM}(g) \mid g \in G\}$ und $\{\mathrm{LM}(g) \mid g \in G\} = \{\mathrm{LM}(h) \mid h \in H\}$.

Beweis.
Die zweite Aussage ist klar mit (c) aus der letzten Proposition. Um die Existenz einer minimalen Gröbnerbasis von I zu zeigen, wähle man zunächst eine beliebige Gröbnerbasis $G \subseteq K[\underline{X}] \setminus \{0\}$ von I. Offensichtlich gibt es $H \subseteq G$ mit

$$(\{\mathrm{LM}(g) \mid g \in G\}) = (\{\mathrm{LM}(h) \mid h \in H\})$$

derart, dass kein Leitmonom eines Elements von H das Leitmonom eines anderen Elements von H teilt.

Satz. Sei $I \subseteq K[\underline{X}]$ ein Ideal. Dann besitzt I eine minimale Gröbnerbasis. Sind G und H zwei minimale Gröbnerbasen von I, so gilt $\#G = \#H = \#\{\mathrm{LM}(g) \mid g \in G\}$ und $\{\mathrm{LM}(g) \mid g \in G\} = \{\mathrm{LM}(h) \mid h \in H\}$.

Beweis.
Die zweite Aussage ist klar mit (c) aus der letzten Proposition. Um die Existenz einer minimalen Gröbnerbasis von I zu zeigen, wähle man zunächst eine beliebige Gröbnerbasis $G \subseteq K[\underline{X}] \setminus \{0\}$ von I. Offensichtlich gibt es $H \subseteq G$ mit

$$(\{\mathrm{LM}(g) \mid g \in G\}) = (\{\mathrm{LM}(h) \mid h \in H\})$$

derart, dass kein Leitmonom eines Elements von H das Leitmonom eines anderen Elements von H teilt. Wegen $(\{\mathrm{LM}(h) \mid h \in H\}) = (\{\mathrm{LM}(g) \mid g \in G\}) = L(I)$ ist auch H eine Gröbnerbasis von I.

Satz. Sei $I \subseteq K[\underline{X}]$ ein Ideal. Dann besitzt I eine minimale Gröbnerbasis. Sind G und H zwei minimale Gröbnerbasen von I, so gilt $\#G = \#H = \#\{\mathrm{LM}(g) \mid g \in G\}$ und $\{\mathrm{LM}(g) \mid g \in G\} = \{\mathrm{LM}(h) \mid h \in H\}$.

Beweis.
Die zweite Aussage ist klar mit (c) aus der letzten Proposition. Um die Existenz einer minimalen Gröbnerbasis von I zu zeigen, wähle man zunächst eine beliebige Gröbnerbasis $G \subseteq K[\underline{X}] \setminus \{0\}$ von I. Offensichtlich gibt es $H \subseteq G$ mit

$$(\{\mathrm{LM}(g) \mid g \in G\}) = (\{\mathrm{LM}(h) \mid h \in H\})$$

derart, dass kein Leitmonom eines Elements von H das Leitmonom eines anderen Elements von H teilt. Wegen $(\{\mathrm{LM}(h) \mid h \in H\}) = (\{\mathrm{LM}(g) \mid g \in G\}) = L(I)$ ist auch H eine Gröbnerbasis von I. Nach der Proposition ist H eine minimale Gröbnerbasis.

Satz. Sei $I \subseteq K[\underline{X}]$ ein Ideal. Dann besitzt I eine minimale Gröbnerbasis. Sind G und H zwei minimale Gröbnerbasen von I, so gilt $\#G = \#H = \#\{\mathrm{LM}(g) \mid g \in G\}$ und $\{\mathrm{LM}(g) \mid g \in G\} = \{\mathrm{LM}(h) \mid h \in H\}$.

Beweis.
Die zweite Aussage ist klar mit (c) aus der letzten Proposition. Um die Existenz einer minimalen Gröbnerbasis von I zu zeigen, wähle man zunächst eine beliebige Gröbnerbasis $G \subseteq K[\underline{X}] \setminus \{0\}$ von I. Offensichtlich gibt es $H \subseteq G$ mit

$$(\{\mathrm{LM}(g) \mid g \in G\}) = (\{\mathrm{LM}(h) \mid h \in H\})$$

derart, dass kein Leitmonom eines Elements von H das Leitmonom eines anderen Elements von H teilt. Wegen $(\{\mathrm{LM}(h) \mid h \in H\}) = (\{\mathrm{LM}(g) \mid g \in G\}) = L(I)$ ist auch H eine Gröbnerbasis von I. Nach der Proposition ist H eine minimale Gröbnerbasis. □

Bemerkung. Es ist jetzt klar, wie man zu einer gegebenen endlichen Menge $F \subseteq K[\underline{X}]$ eine minimale Gröbnerbasis H von (F) berechnet.

Reduzierte Gröbnerbasen

Definition.

(a) Ein Polynom $f \in K[\underline{X}]$ heißt normiert (bezüglich $\leq$), wenn $f \neq 0$ und $\mathrm{LC}(f) = 1$.

Reduzierte Gröbnerbasen

Definition.

(a) Ein Polynom $f \in K[\underline{X}]$ heißt normiert (bezüglich $\leq$), wenn $f \neq 0$ und $\mathrm{LC}(f) = 1$.

(b) Eine Menge $F \subseteq K[\underline{X}]$ heißt normiert (bezüglich $\leq$), wenn jedes ihrer Elemente normiert ist.

Reduzierte Gröbnerbasen

Definition.

(a) Ein Polynom $f \in K[\underline{X}]$ heißt normiert (bezüglich $\leq$), wenn $f \neq 0$ und $\mathrm{LC}(f) = 1$.

(b) Eine Menge $F \subseteq K[\underline{X}]$ heißt normiert (bezüglich $\leq$), wenn jedes ihrer Elemente normiert ist.

(c) Eine Menge $F \subseteq K[\underline{X}]$ heißt reduziert (bezüglich $\leq$), wenn F normiert ist und jedes $f \in F$ reduziert modulo $F \setminus \{f\}$ ist.

Reduzierte Gröbnerbasen

Definition.

(a) Ein Polynom $f \in K[\underline{X}]$ heißt normiert (bezüglich $\leq$), wenn $f \neq 0$ und $\mathrm{LC}(f) = 1$.

(b) Eine Menge $F \subseteq K[\underline{X}]$ heißt normiert (bezüglich $\leq$), wenn jedes ihrer Elemente normiert ist.

(c) Eine Menge $F \subseteq K[\underline{X}]$ heißt reduziert (bezüglich $\leq$), wenn F normiert ist und jedes $f \in F$ reduziert modulo $F \setminus \{f\}$ ist.

Proposition. Jede reduzierte Gröbnerbasis ist minimal.

Satz. Jedes Ideal von $K[\underline{X}]$ besitzt eine eindeutig bestimmte reduzierte Gröbnerbasis.

Beweis.
Sei $I \subseteq K[\underline{X}]$ ein Ideal.

Satz. Jedes Ideal von $K[\underline{X}]$ besitzt eine eindeutig bestimmte reduzierte Gröbnerbasis.

Beweis.
Sei $I \subseteq K[\underline{X}]$ ein Ideal.

Eindeutigkeit Seien G und H reduzierte Gröbnerbasen von I. Da G und H nach der letzten Proposition minimal sind,

Satz. Jedes Ideal von $K[\underline{X}]$ besitzt eine eindeutig bestimmte reduzierte Gröbnerbasis.

Beweis.
Sei $I \subseteq K[\underline{X}]$ ein Ideal.

Eindeutigkeit Seien G und H reduzierte Gröbnerbasen von I. Da G und H nach der letzten Proposition minimal sind, gilt nach dem letzten Satz $\#G = \#H = \#\{\mathrm{LM}(g) \mid g \in G\}$ und

$$(*) \qquad \{\mathrm{LM}(g) \mid g \in G\} = \{\mathrm{LM}(h) \mid h \in H\}.$$

Satz. Jedes Ideal von $K[\underline{X}]$ besitzt eine eindeutig bestimmte reduzierte Gröbnerbasis.

Beweis.
Sei $I \subseteq K[\underline{X}]$ ein Ideal.

Eindeutigkeit Seien G und H reduzierte Gröbnerbasen von I. Da G und H nach der letzten Proposition minimal sind, gilt nach dem letzten Satz $\#G = \#H = \#\{\mathrm{LM}(g) \mid g \in G\}$ und

$$(*) \qquad \{\mathrm{LM}(g) \mid g \in G\} = \{\mathrm{LM}(h) \mid h \in H\}.$$

Sei $g \in G$. Es reicht $g \in H$ zu zeigen. Wähle $h \in H$ mit $u := \mathrm{LM}(g) = \mathrm{LM}(h)$. Wir behaupten $g = h$.

□

Satz. Jedes Ideal von $K[\underline{X}]$ besitzt eine eindeutig bestimmte reduzierte Gröbnerbasis.

Beweis.
Sei $I \subseteq K[\underline{X}]$ ein Ideal.

Eindeutigkeit Seien G und H reduzierte Gröbnerbasen von I. Da G und H nach der letzten Proposition minimal sind, gilt nach dem letzten Satz $\#G = \#H = \#\{\mathrm{LM}(g) \mid g \in G\}$ und

$$(*) \qquad \{\mathrm{LM}(g) \mid g \in G\} = \{\mathrm{LM}(h) \mid h \in H\}.$$

Sei $g \in G$. Es reicht $g \in H$ zu zeigen. Wähle $h \in H$ mit $u := \mathrm{LM}(g) = \mathrm{LM}(h)$. Wir behaupten $g = h$. Wegen $(*)$ gilt offenbar $\mathrm{red}(G) = \mathrm{red}(H)$.

□

Satz. Jedes Ideal von $K[\underline{X}]$ besitzt eine eindeutig bestimmte reduzierte Gröbnerbasis.

Beweis.
Sei $I \subseteq K[\underline{X}]$ ein Ideal.

Eindeutigkeit Seien G und H reduzierte Gröbnerbasen von I. Da G und H nach der letzten Proposition minimal sind, gilt nach dem letzten Satz $\#G = \#H = \#\{\mathrm{LM}(g) \mid g \in G\}$ und

$$(*) \qquad \{\mathrm{LM}(g) \mid g \in G\} = \{\mathrm{LM}(h) \mid h \in H\}.$$

Sei $g \in G$. Es reicht $g \in H$ zu zeigen. Wähle $h \in H$ mit $u := \mathrm{LM}(g) = \mathrm{LM}(h)$. Wir behaupten $g = h$. Wegen $(*)$ gilt offenbar $\mathrm{red}(G) = \mathrm{red}(H)$. Wegen $g \in \mathrm{red}(G \setminus \{g\})$ gilt $M(g) \setminus \{u\} \subseteq \mathrm{red}(G)$.

□

Satz. Jedes Ideal von $K[\underline{X}]$ besitzt eine eindeutig bestimmte reduzierte Gröbnerbasis.

Beweis.
Sei $I \subseteq K[\underline{X}]$ ein Ideal.

Eindeutigkeit Seien G und H reduzierte Gröbnerbasen von I. Da G und H nach der letzten Proposition minimal sind, gilt nach dem letzten Satz $\#G = \#H = \#\{\mathrm{LM}(g) \mid g \in G\}$ und

$$(*) \qquad \{\mathrm{LM}(g) \mid g \in G\} = \{\mathrm{LM}(h) \mid h \in H\}.$$

Sei $g \in G$. Es reicht $g \in H$ zu zeigen. Wähle $h \in H$ mit $u := \mathrm{LM}(g) = \mathrm{LM}(h)$. Wir behaupten $g = h$. Wegen $(*)$ gilt offenbar $\mathrm{red}(G) = \mathrm{red}(H)$. Wegen $g \in \mathrm{red}(G \setminus \{g\})$ gilt $M(g) \setminus \{u\} \subseteq \mathrm{red}(G)$.
Analog $M(h) \setminus \{u\} \subseteq \mathrm{red}(H)$.

□

Satz. Jedes Ideal von $K[\underline{X}]$ besitzt eine eindeutig bestimmte reduzierte Gröbnerbasis.

Beweis.
Sei $I \subseteq K[\underline{X}]$ ein Ideal.

Eindeutigkeit Seien G und H reduzierte Gröbnerbasen von I. Da G und H nach der letzten Proposition minimal sind, gilt nach dem letzten Satz $\#G = \#H = \#\{\mathrm{LM}(g) \mid g \in G\}$ und

$$(*) \qquad \{\mathrm{LM}(g) \mid g \in G\} = \{\mathrm{LM}(h) \mid h \in H\}.$$

Sei $g \in G$. Es reicht $g \in H$ zu zeigen. Wähle $h \in H$ mit $u := \mathrm{LM}(g) = \mathrm{LM}(h)$. Wir behaupten $g = h$. Wegen $(*)$ gilt offenbar $\mathrm{red}(G) = \mathrm{red}(H)$. Wegen $g \in \mathrm{red}(G \setminus \{g\})$ gilt $M(g) \setminus \{u\} \subseteq \mathrm{red}(G)$.
Analog $M(h) \setminus \{u\} \subseteq \mathrm{red}(H)$. Da g und h normiert sind, haben wir $M(g - h) \subseteq (M(g) \cup M(h)) \setminus \{u\} \subseteq \mathrm{red}(G) = \mathrm{red}(H)$ und daher $g - h \in \mathrm{red}(G)$.

□

Satz. Jedes Ideal von $K[\underline{X}]$ besitzt eine eindeutig bestimmte reduzierte Gröbnerbasis.

Beweis.
Sei $I \subseteq K[\underline{X}]$ ein Ideal.

Eindeutigkeit Seien G und H reduzierte Gröbnerbasen von I. Da G und H nach der letzten Proposition minimal sind, gilt nach dem letzten Satz $\#G = \#H = \#\{\mathrm{LM}(g) \mid g \in G\}$ und

$$(*) \qquad \{\mathrm{LM}(g) \mid g \in G\} = \{\mathrm{LM}(h) \mid h \in H\}.$$

Sei $g \in G$. Es reicht $g \in H$ zu zeigen. Wähle $h \in H$ mit $u := \mathrm{LM}(g) = \mathrm{LM}(h)$. Wir behaupten $g = h$. Wegen $(*)$ gilt offenbar $\mathrm{red}(G) = \mathrm{red}(H)$. Wegen $g \in \mathrm{red}(G \setminus \{g\})$ gilt $M(g) \setminus \{u\} \subseteq \mathrm{red}(G)$.
Analog $M(h) \setminus \{u\} \subseteq \mathrm{red}(H)$. Da g und h normiert sind, haben wir $M(g-h) \subseteq (M(g) \cup M(h)) \setminus \{u\} \subseteq \mathrm{red}(G) = \mathrm{red}(H)$ und daher $g - h \in \mathrm{red}(G)$. Andererseits $g - h \in I$ und daher $g - h \xrightarrow[G]{*} 0$.

□

Satz. Jedes Ideal von $K[\underline{X}]$ besitzt eine eindeutig bestimmte reduzierte Gröbnerbasis.

Beweis.
Sei $I \subseteq K[\underline{X}]$ ein Ideal.

Eindeutigkeit Seien G und H reduzierte Gröbnerbasen von I. Da G und H nach der letzten Proposition minimal sind, gilt nach dem letzten Satz $\#G = \#H = \#\{\mathrm{LM}(g) \mid g \in G\}$ und

$$(*) \qquad \{\mathrm{LM}(g) \mid g \in G\} = \{\mathrm{LM}(h) \mid h \in H\}.$$

Sei $g \in G$. Es reicht $g \in H$ zu zeigen. Wähle $h \in H$ mit $u := \mathrm{LM}(g) = \mathrm{LM}(h)$. Wir behaupten $g = h$. Wegen $(*)$ gilt offenbar $\mathrm{red}(G) = \mathrm{red}(H)$. Wegen $g \in \mathrm{red}(G \setminus \{g\})$ gilt $M(g) \setminus \{u\} \subseteq \mathrm{red}(G)$.
Analog $M(h) \setminus \{u\} \subseteq \mathrm{red}(H)$. Da g und h normiert sind, haben wir $M(g-h) \subseteq (M(g) \cup M(h)) \setminus \{u\} \subseteq \mathrm{red}(G) = \mathrm{red}(H)$ und daher $g - h \in \mathrm{red}(G)$. Andererseits $g - h \in I$ und daher $g - h \xrightarrow[G]{*} 0$.
Es folgt $g - h = 0$, also $g = h \in H$.

□

Satz. Jedes Ideal von $K[\underline{X}]$ besitzt eine eindeutig bestimmte reduzierte Gröbnerbasis.

Beweis.
Sei $I \subseteq K[\underline{X}]$ ein Ideal.

Existenz Wähle mit dem letzten Satz eine minimale Gröbnerbasis G von I. Wähle zu jedem $g \in G$ ein $g' \in \mathrm{red}(G \setminus \{g\})$ mit $g \xrightarrow[G\setminus\{g\}]{*} g'$.

Satz. Jedes Ideal von $K[\underline{X}]$ besitzt eine eindeutig bestimmte reduzierte Gröbnerbasis.

Beweis.
Sei $I \subseteq K[\underline{X}]$ ein Ideal.

Existenz Wähle mit dem letzten Satz eine minimale Gröbnerbasis G von I. Wähle zu jedem $g \in G$ ein $g' \in \mathrm{red}(G \setminus \{g\})$ mit $g \xrightarrow[G\setminus\{g\}]{*} g'$.

Wegen der Minimalität von G gilt $\mathrm{LM}(g') = \mathrm{LM}(g)$ für alle $g \in G$.

Satz. Jedes Ideal von $K[\underline{X}]$ besitzt eine eindeutig bestimmte reduzierte Gröbnerbasis.

Beweis.
Sei $I \subseteq K[\underline{X}]$ ein Ideal.

Existenz Wähle mit dem letzten Satz eine minimale Gröbnerbasis G von I. Wähle zu jedem $g \in G$ ein $g' \in \mathrm{red}(G \setminus \{g\})$ mit $g \xrightarrow[G\setminus\{g\}]{*} g'$.

Wegen der Minimalität von G gilt $\mathrm{LM}(g') = \mathrm{LM}(g)$ für alle $g \in G$.
Mit G ist auch $H := \{g' \mid g \in G\}$ eine Gröbnerbasis von I.

□

Satz. Jedes Ideal von $K[\underline{X}]$ besitzt eine eindeutig bestimmte reduzierte Gröbnerbasis.

Beweis.
Sei $I \subseteq K[\underline{X}]$ ein Ideal.

Existenz Wähle mit dem letzten Satz eine minimale Gröbnerbasis G von I. Wähle zu jedem $g \in G$ ein $g' \in \mathrm{red}(G \setminus \{g\})$ mit $g \xrightarrow[G\setminus\{g\}]{*} g'$.

Wegen der Minimalität von G gilt $\mathrm{LM}(g') = \mathrm{LM}(g)$ für alle $g \in G$. Mit G ist auch $H := \{g' \mid g \in G\}$ eine Gröbnerbasis von I. Man sieht $\mathrm{red}(G \setminus \{g\}) = \mathrm{red}(H \setminus \{g'\})$ für alle $g \in G$.

□

Satz. Jedes Ideal von $K[\underline{X}]$ besitzt eine eindeutig bestimmte reduzierte Gröbnerbasis.

Beweis.
Sei $I \subseteq K[\underline{X}]$ ein Ideal.

Existenz Wähle mit dem letzten Satz eine minimale Gröbnerbasis G von I. Wähle zu jedem $g \in G$ ein $g' \in \mathrm{red}(G \setminus \{g\})$ mit $g \xrightarrow[G\setminus\{g\}]{*} g'$.

Wegen der Minimalität von G gilt $\mathrm{LM}(g') = \mathrm{LM}(g)$ für alle $g \in G$. Mit G ist auch $H := \{g' \mid g \in G\}$ eine Gröbnerbasis von I. Man sieht $\mathrm{red}(G \setminus \{g\}) = \mathrm{red}(H \setminus \{g'\})$ für alle $g \in G$. Somit $g' \in \mathrm{red}(H \setminus \{g'\})$ für alle $g \in G$, das heißt H ist reduziert.

Interreduktionsalgorithmus

Eingabe: $F \subseteq K[\underline{X}]$ endlich

Ausgabe: $G \subseteq K[\underline{X}]$ endlich und reduziert mit $(G) = (F)$ derart, dass G eine Gröbnerbasis ist, falls F eine ist.

Interreduktionsalgorithmus

Eingabe: $F \subseteq K[\underline{X}]$ endlich

Ausgabe: $G \subseteq K[\underline{X}]$ endlich und reduziert mit $(G) = (F)$ derart, dass G eine Gröbnerbasis ist, falls F eine ist.

$G \leftarrow F$;

solange es $g \in G$ gibt mit $g \notin \mathrm{red}(G \setminus \{g\})$

$\big($wähle $g \in G$ mit $g \notin \mathrm{red}(G \setminus \{g\})$;

wähle $h \in K[\underline{X}]$ mit $g \underset{G\setminus\{g\}}{\longrightarrow} h$; $G \leftarrow (G \setminus \{g\}) \cup \{h\}\big)$;

$G \leftarrow \{\frac{g}{\mathrm{LC}(g)} \mid g \in G \setminus \{0\}\}$

Interreduktionsalgorithmus

Eingabe: $F \subseteq K[\underline{X}]$ endlich

Ausgabe: $G \subseteq K[\underline{X}]$ endlich und reduziert mit $(G) = (F)$ derart, dass G eine Gröbnerbasis ist, falls F eine ist.

$G \leftarrow F$;

solange es $g \in G$ gibt mit $g \notin \mathrm{red}(G \setminus \{g\})$

$\big($wähle $g \in G$ mit $g \notin \mathrm{red}(G \setminus \{g\})$;

wähle $h \in K[\underline{X}]$ mit $g \underset{G\setminus\{g\}}{\longrightarrow} h$; $G \leftarrow (G \setminus \{g\}) \cup \{h\}\big)$;

$G \leftarrow \{\frac{g}{\mathrm{LC}(g)} \mid g \in G \setminus \{0\}\}$

Beweis. Terminierung Angenommen der Algorithmus terminiert nicht. Wähle dann $s \in \mathbb{N}$ und $g_1^{(0)}, \ldots, g_s^{(0)} \in K[\underline{X}]$ mit $F = \{g_1^{(0)}, \ldots, g_s^{(0)}\}$. Dann gilt zu Beginn des ersten Schleifendurchlaufs $G = \{g_1^{(0)}, \ldots, g_s^{(0)}\}$. Wir nehmen an zu Beginn des i-ten Durchlaufs ($i \in \mathbb{N}$) gelte $G = \{g_1^{(i-1)}, \ldots, g_s^{(i-1)}\}$ für schon definierte $g_1^{(i-1)}, \ldots, g_s^{(i-1)} \in K[\underline{X}]$. [...]

Interreduktionsalgorithmus

Eingabe: $F \subseteq K[\underline{X}]$ endlich

Ausgabe: $G \subseteq K[\underline{X}]$ endlich und reduziert mit $(G) = (F)$ derart, dass G eine Gröbnerbasis ist, falls F eine ist.

$G \leftarrow F$;

solange es $g \in G$ gibt mit $g \notin \mathrm{red}(G \setminus \{g\})$

$\big($wähle $g \in G$ mit $g \notin \mathrm{red}(G \setminus \{g\})$;

wähle $h \in K[\underline{X}]$ mit $g \underset{G\setminus\{g\}}{\longrightarrow} h$; $G \leftarrow (G \setminus \{g\}) \cup \{h\}\big)$;

$G \leftarrow \{\frac{g}{\mathrm{LC}(g)} \mid g \in G \setminus \{0\}\}$

Beweis. Korrektheit Schleifeninvarianten:

(a) $G \subseteq K[\underline{X}]$ ist endlich mit $(G) = (F)$.

(b) G ist eine Gröbnerbasis, falls F eine war.

Für (a) ist das schnell zu sehen. Für (b) reicht es zu zeigen, dass $L(I) = (\{\mathrm{LM}(f) \mid f \in G \setminus \{0\}\})$ mit $I := (F)$ eine Invariante ist. [...] $\square$

Bemerkung. Wie versprochen sehen wir jetzt, dass Gröbnerbasen gleichzeitig den euklidischen Algorithmus für Polynome in einer Variablen als auch den Gauß-Algorithmus für lineare Polynome verallgemeinern:

Bemerkung. Wie versprochen sehen wir jetzt, dass Gröbnerbasen gleichzeitig den euklidischen Algorithmus für Polynome in einer Variablen als auch den Gauß-Algorithmus für lineare Polynome verallgemeinern: Seien nämlich $f_1, \ldots, f_s \in K[\underline{X}]$ und $I := (f_1, \ldots, f_s)$.

Bemerkung. Wie versprochen sehen wir jetzt, dass Gröbnerbasen gleichzeitig den euklidischen Algorithmus für Polynome in einer Variablen als auch den Gauß-Algorithmus für lineare Polynome verallgemeinern: Seien nämlich $f_1, \ldots, f_s \in K[\underline{X}]$ und $I := (f_1, \ldots, f_s)$.

(a) Gelte $n = 1$, also $\underline{X} = X$. Dann gibt es genau ein $g \in K[\underline{X}]$ mit $I = (g)$ und g normiert oder $g = 0$. Dann ist $\{g\} \setminus \{0\}$ die eindeutig bestimmte reduzierte Gröbnerbasis von I.

Bemerkung. Wie versprochen sehen wir jetzt, dass Gröbnerbasen gleichzeitig den euklidischen Algorithmus für Polynome in einer Variablen als auch den Gauß-Algorithmus für lineare Polynome verallgemeinern: Seien nämlich $f_1, \ldots, f_s \in K[\underline{X}]$ und $I := (f_1, \ldots, f_s)$.

(b) Gelte $\deg f_i \leq 1$ für alle $i \in \{1, \ldots, s\}$. Dann gibt es eindeutig bestimmte

$$g_i = \sum_{j=1}^{n} a_{ij} X_j + b_i \qquad (i \in \{1, \ldots, s\}, a_{ij}, b_i \in K)$$

derart, dass mit $A := (a_{ij})_{1 \leq i \leq s, 1 \leq j \leq n}$ die Matrix $(A\ b) \in K^{s \times (n+1)}$ in reduzierter Stufenform ist und

$$Kf_1 + \ldots + Kf_s = Kg_1 + \ldots + Kg_s.$$

Bemerkung. Wie versprochen sehen wir jetzt, dass Gröbnerbasen gleichzeitig den euklidischen Algorithmus für Polynome in einer Variablen als auch den Gauß-Algorithmus für lineare Polynome verallgemeinern: Seien nämlich $f_1, \ldots, f_s \in K[\underline{X}]$ und $I := (f_1, \ldots, f_s)$.

(b) Gelte $\deg f_i \leq 1$ für alle $i \in \{1, \ldots, s\}$. Dann gibt es eindeutig bestimmte

$$g_i = \sum_{j=1}^{n} a_{ij} X_j + b_i \qquad (i \in \{1, \ldots, s\}, a_{ij}, b_i \in K)$$

derart, dass mit $A := (a_{ij})_{1 \leq i \leq s, 1 \leq j \leq n}$ die Matrix $(A\ b) \in K^{s \times (n+1)}$ in reduzierter Stufenform ist und

$$Kf_1 + \ldots + Kf_s = Kg_1 + \ldots + Kg_s.$$

Ist $\leq$ eine Termordnung mit $X_1 \geq X_2 \geq \cdots \geq X_n$, so ist im Fall $1 \notin \{g_1, \ldots, g_s\}$ die Menge $\{g_1, \ldots, g_s\} \setminus \{0\}$ und sonst $\{1\}$ eine reduzierte Gröbnerbasis von I. Dies sieht man mit dem Buchberger-Kriterium zusammen mit dem folgenden Lemma.

Lemma. Seien $f, g \in K[\underline{X}] \setminus \{0\}$ derart, dass kein X_i gleichzeitig $\mathrm{LM}(f)$ und $\mathrm{LM}(g)$ teilt. Dann $\mathrm{spol}(f, g) \xrightarrow[\{f,g\}]{*} 0$.

Lemma. Seien $f, g \in K[\underline{X}] \setminus \{0\}$ derart, dass kein X_i gleichzeitig $\mathrm{LM}(f)$ und $\mathrm{LM}(g)$ teilt. Dann $\mathrm{spol}(f, g) \xrightarrow[\{f,g\}]{*} 0$.

Beweis.
Schreibe $f = \sum_{i=1}^{k} a_i u_i$ und $g = \sum_{j=1}^{\ell} b_j v_j$ mit $k, \ell \in \mathbb{N}$, $a_i, b_j \in K^\times$ und $u_i, v_j \in [\underline{X}]$, wobei $u_1 > \ldots > u_k$ und $v_1 > \ldots > v_\ell$ gelte.

Lemma. Seien $f, g \in K[\underline{X}] \setminus \{0\}$ derart, dass kein X_i gleichzeitig $\mathrm{LM}(f)$ und $\mathrm{LM}(g)$ teilt. Dann $\mathrm{spol}(f,g) \xrightarrow[\{f,g\}]{*} 0$.

Beweis.
Schreibe $f = \sum_{i=1}^{k} a_i u_i$ und $g = \sum_{j=1}^{\ell} b_j v_j$ mit $k, \ell \in \mathbb{N}$, $a_i, b_j \in K^\times$ und $u_i, v_j \in [\underline{X}]$, wobei $u_1 > \ldots > u_k$ und $v_1 > \ldots > v_\ell$ gelte.
Nach Voraussetzung gilt $\mathrm{lcm}(u_1, v_1) = u_1 v_1$ und daher

$$\mathrm{spol}(f,g) = b_1 v_1 f - a_1 u_1 g = \underbrace{b_1 v_1 \sum_{i=2}^{k} a_i u_i}_{=:p} - \underbrace{a_1 u_1 \sum_{j=2}^{\ell} b_j v_j}_{=:q}.$$

Lemma. Seien $f, g \in K[\underline{X}] \setminus \{0\}$ derart, dass kein X_i gleichzeitig $\mathrm{LM}(f)$ und $\mathrm{LM}(g)$ teilt. Dann $\mathrm{spol}(f,g) \xrightarrow[\{f,g\}]{*} 0$.

Beweis.
Schreibe $f = \sum_{i=1}^{k} a_i u_i$ und $g = \sum_{j=1}^{\ell} b_j v_j$ mit $k, \ell \in \mathbb{N}$, $a_i, b_j \in K^\times$ und $u_i, v_j \in [\underline{X}]$, wobei $u_1 > \ldots > u_k$ und $v_1 > \ldots > v_\ell$ gelte.
Nach Voraussetzung gilt $\mathrm{lcm}(u_1, v_1) = u_1 v_1$ und daher

$$\mathrm{spol}(f,g) = b_1 v_1 f - a_1 u_1 g = \underbrace{b_1 v_1 \sum_{i=2}^{k} a_i u_i}_{=:p} - \underbrace{a_1 u_1 \sum_{j=2}^{\ell} b_j v_j}_{=:q}.$$

Es gilt $M(p) \cap M(q) = \emptyset$, denn sonst gäbe es $i \in \{2, \ldots, k\}$ und $j \in \{2, \ldots, \ell\}$ mit $v_1 u_i = u_1 v_j$ und es gälte $u_1 v_1 = \mathrm{lcm}(u_1, v_1) \mid v_1 u_i$ und damit $u_1 v_1 \leq v_1 u_i \leq v_1 u_1 = u_1 v_1$, was $u_1 v_1 = u_i v_1$ also $u_1 = u_i$ implizierte $\lightning$.

Lemma. Seien $f, g \in K[\underline{X}] \setminus \{0\}$ derart, dass kein X_i gleichzeitig $\mathrm{LM}(f)$ und $\mathrm{LM}(g)$ teilt. Dann $\mathrm{spol}(f,g) \xrightarrow[\{f,g\}]{*} 0$.

Beweis.
Schreibe $f = \sum_{i=1}^{k} a_i u_i$ und $g = \sum_{j=1}^{\ell} b_j v_j$ mit $k, \ell \in \mathbb{N}$, $a_i, b_j \in K^\times$ und $u_i, v_j \in [\underline{X}]$, wobei $u_1 > \ldots > u_k$ und $v_1 > \ldots > v_\ell$ gelte.
Nach Voraussetzung gilt $\mathrm{lcm}(u_1, v_1) = u_1 v_1$ und daher

$$\mathrm{spol}(f,g) = b_1 v_1 f - a_1 u_1 g = \underbrace{b_1 v_1 \sum_{i=2}^{k} a_i u_i}_{=:p} - \underbrace{a_1 u_1 \sum_{j=2}^{\ell} b_j v_j}_{=:q}.$$

Es gilt $M(p) \cap M(q) = \emptyset$, denn sonst gäbe es $i \in \{2, \ldots, k\}$ und $j \in \{2, \ldots, \ell\}$ mit $v_1 u_i = u_1 v_j$ und es gälte $u_1 v_1 = \mathrm{lcm}(u_1, v_1) \mid v_1 u_i$ und damit $u_1 v_1 \leq v_1 u_i \leq v_1 u_1 = u_1 v_1$, was $u_1 v_1 = u_i v_1$ also $u_1 = u_i$ implizierte $\lightning$. Jedes der $\ell - 1$ Monome von q ist also ein Monom von $\mathrm{spol}(f,g)$ und wird von $u_1 = \mathrm{LM}(f)$ geteilt. Wir addieren nun nacheinander $b_\ell v_\ell f, b_{\ell-1} v_{\ell-1} f, \ldots, b_2 v_2 f$ zu $\mathrm{spol}(f,g)$ und überlegen uns, dass dies jeweils ein Reduktionsschritt modulo f ist [...] □