10.22 Satz

Sei $L \supset \mathbb{Q}$ ein Oberkörper mit abzählbarer Transzendenzbasis, $\operatorname{trdeg}_{\mathbb{Q}} L \leq |\mathbb{N}|$

Dann existiert die Einbettung $L \hookrightarrow \mathbb{C}$ als Unterkörper.

~~Z~~ zeigen zunächst, dass auch L abzählbar ist.

10.23 Satz

1) Sei $\mathbb{Q}(B) \supset \mathbb{Q}$ eine durch die abzählbare Menge B erzeugte Körpererweiterung. Dann ist auch $\mathbb{Q}(B)$ abzählbar. 2) Insbesondere gilt

$$|\mathbb{N}| < \operatorname{trdeg}_{\mathbb{Q}} \mathbb{C} \leq |\mathbb{C}|$$

Beweis:

1) Sei $K(b) \supset K$ eine primitive Körpererweiterung. Dann ist mit K auch $K(b)$ abzählbar.

Bew: Ist b algebraisch, n der Grad des Minimalpolynoms. Dann ist $K(b) = K[b] \cong K^n$ als K-Vektorraum. Also ist K ebenfalls abzählbar.

Ist b transzendent, dann ist $K[b] \cong K[x] = \bigcup_{n=0}^{\infty} \{f \in K[x] \mid \deg f \leq n\}$ abzählbar als abz. Vereinigung abzählbarer Mengen.

$K(b) \cong K(x)$ ist das Bild von

$$\begin{aligned} K[x] \times K[x] \setminus \{0\} &\to K(x) \\ (f, g) &\longmapsto \frac{f}{g} \end{aligned}$$

also das Bild einer abzählbaren Menge.

2) Mit K ist auch $K(b_1, \dots, b_n)$ abzählbar, per Induktion K abzählbar $\Rightarrow K(b_1)$ abz. usw.

3) Sei $B = \{b_i\}_{i \in \mathbb{N}}$ eine Abzählung $K(B) = \bigcup_{i=0}^{\infty} K(b_0, \dots, b_i)$, K ist also auch abzählbar

4) Der alg. Abschluss $\overline{K}$ eines abzählbaren Körpers K ist abzählbar

$$\overline{K} = \bigcup_{f \in K[x]} \{a \in \overline{K} \mid f(a) = 0\}$$

Es folgt $|\mathbb{N}| < \operatorname{trdeg}_{\mathbb{Q}} \mathbb{C}$ da andernfalls $\mathbb{C}$ abzählbar wäre.

Beweis von 10.22

Sei B eine Transzendenzbasis von L über $\mathbb{Q}$, also abzählbar und C eine Transzendenzbasis von $\mathbb{C}$ über $\mathbb{Q}$. Dann können wir eine zu B gleichmächtige Teilmenge $C' \subset C$ finden $\mathbb{Q}(B) \cong \mathbb{Q}(C') \subset \mathbb{C}$

Der algebraische Schluss von $\mathbb{Q}(C')$ können wir als Abschluss von $\mathbb{Q}(C')$ in $\mathbb{C}$ realisieren

$$\mathbb{Q}(b) \hookrightarrow \overline{\mathbb{Q}(C')} \subset \mathbb{C}$$

Diese können wir entlang der algebraischen Körpererw. $\mathbb{Q}(B) \subset L$ zu einem Körperhom. $L \hookrightarrow \overline{\mathbb{Q}(C')} \subset \mathbb{C}$ fortsetzen $\square$

§ 11 Gröbnerbasen

Motivation: K Körper. In $\frac{K[x]}{(f)}$ rechnen wir wie folgt: Als Basis des K-Vektorraums sind die Monomen $1, x, \dots, x^{n-1}$ wobei $n = \deg f$.
Für die Multiplikation multiplizieren wir die Repräsentanten und gehen zum Rest nach Division mit f über.

$$\mathbb{C} = \frac{\mathbb{R}[x]}{x^2+1}$$

Wie rechnet man in $K[x_1, \dots, x_n]/I$ mit $I = \langle f_1, \dots, f_r \rangle$?

Bsp $f_1 = x^2 + xy \in K[x,y]$
Division nach f erlaubt es in beliebigen Polynomen alle Monome, die durch x^2 teilbar sind zu eliminieren. Genauso für $f_2 = y^2 + xy$ können wir alle Monome, die durch y^2 teilbar sind eliminieren.

Frage: Können wir mit f_1 und f_2 alle Monome, die durch x^2 oder y^2 teilbar sind eliminieren. $I = \langle f_1, f_2 \rangle$

$$x^2y \equiv -xy^2 \pmod{f_1}$$
$$\equiv x^2y \pmod{f_2}$$

Antwort ist nein, denn wäre dem nicht so, dann wären $\overline{1}, \overline{x}, \overline{y}, \overline{xy}$ ein K-Vektorraum Erzeugendensystem von $\frac{K[x,y]}{\langle f_1, f_2 \rangle}$ bilden.

Aber $\frac{K[x,y]}{\langle f_1, f_2 \rangle} \to \frac{K[x,y]}{\langle x+y \rangle} \cong K[y]$ nicht endlich dim. als K VR

Was ist schiefgegangen?

$$\underset{\text{Leitterm}}{\underset{\uparrow}{x^2}} + xy \qquad \underset{\text{Leitterm}}{\underset{\uparrow}{y^2}} + xy$$

11.1 Def Sei $P = K[x_1, \dots, x_n]$ ein Polynomring. Ein Monom in P ist ein Ausdruck $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ $\alpha \in \mathbb{N}^n$.
Ein Term in P ist Ausdruck cx^α, $c \in K$ jedes Polynom ist dann eine endl. Summe von Termen $f = \sum_{\alpha \in \mathbb{N}^n} f_\alpha x^\alpha$; fast alle $f_\alpha = 0 \in K$

Eine Monomordnung auf P ist eine vollständige Ordnung der Monome, die $x^\alpha \geq x^\beta \Rightarrow x^\alpha x^\gamma \geq x^\beta x^\gamma$ $\forall$ Monome $x^\alpha, x^\beta, x^\gamma$

Eine Monomordnung heißt global, wenn $x_i > 1$ für $i = 1, \dots, n$

Gegeben sei eine Monomordnung. Dann ist der Leitterm eines Polynoms $f = \sum f_\alpha x^\alpha$ der Term $\underset{\text{initial term}}{in(f)} = f_\beta x^\beta$, wobei $x^\beta = \max\{x^\alpha \mid f_\alpha \neq 0\}$

Beispiele 1) $>_{lex}$ lexikographisch

$x^\alpha > x^\beta$ falls für i mit $\alpha_j = \beta_j$ für $j < i$ $\alpha_i > \beta_i$ gilt

$\underbrace{x_1 x_1 \cdots}_{\alpha_1} \underbrace{x_2 \cdots x_2}_{\alpha_2} \cdots \underbrace{x_n}$ die Monome werden wie im Lexikon angeordnet

2) $(w_1, \dots, w_n) = w$ $\mathbb{Q}$-linear unabh. pos. Gewichte

$x^\alpha >_w x^\beta \iff L_w : \mathbb{R}^n \to \mathbb{R}$ $(a_1, \dots, a_n) \mapsto \sum w_i a_i$

$L(\alpha) > L(\beta)$

3) rückwärtslexographisch $x^\alpha >_{rlex} x^\beta$ falls $|\alpha|_i = \sum_{i=1}^n \alpha_i > |\beta|$ oder $|\alpha| = |\beta|$

und für das letzte i für das $\alpha_i \neq \beta_i$ gilt die Ungleichung

$\alpha_i < \beta_i$ erfüllt ist

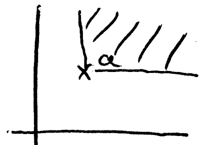
Bsp: $x > y > z$ $\quad x^2 >_{rlex} xy >_{rlex} y^2 >_{rlex} xz >_{rlex} yz >_{rlex} z^2 \quad x^2 >_{lex} xy >_{lex} xz >_{lex} y^2 >_{lex} yz >_{lex} z^2$

11.2 **Lemma** Sei $>$ eine globale Monomordnung auf $K[x_1, \dots, x_n]$

Jede nichtleere Menge von Monomen hat ein kleinstes Element.

Beweis: $\{x^a \mid a \in A\}$ $A \subset \mathbb{N}^n$

Da $>$ global ist, ist das kleinste Element von $\{x^a \mid a \in A\}$ mit dem kleinsten Monom in dem monomialen Ideal $\langle x^a \mid a \in A \rangle \subset k[x_1, \dots, x_n]$ identisch.



$\mathbb{N}^n$

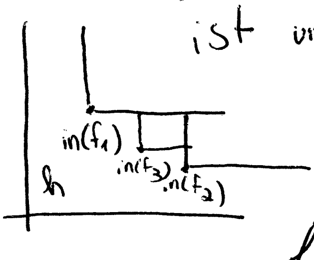
Da monomiale Ideale endlich erzeugt sind (wie jedes Ideal) ist das kleinste Element unter den endlich vielen Erzeugern.

11.3 **Satz** (Division mit Rest)

Sei $>$ eine globale Monomordnung auf $P = K[x_1, \dots, x_n]$ $f_1, \dots, f_n \in P$ und f ein weiteres Polynom. Dann gibt es ~~eind~~ eindeutig bestimmte $g_1, \dots, g_r \in P$ und $h \in P$ so dass

1) $f = g_1 f_1 + \dots + g_r f_r + h$

2) Kein Term von $g_i\, in(f_i)$ durch Term $in(f_j)$ für ein $j < i$ teilbar ist und kein Term von h durch einen Leitterm $in(f_i)$ $i = 1, \dots, r$ teilbar ist.



Bew: Die Existenzaussage ist offensichtlich wenn $f_1, \dots, f_r$ Monome sind. Im Allgemeinen schreiben wir

$f = \tilde{g}_1\, in(f_1) + \dots + \tilde{g}_r\, in(f_r) + \tilde{h}$ so dass 2) erfüllt ist

und betrachten $\tilde{f} = f - \sum_{i=1}^r \tilde{g}_i f_i - \tilde{h}$.

Wegen 2) ~~sind~~ haben die Initialformen $in\, g_i\, in(f_i)$ und $in(h)$ verschiedene Monome

Also $in(\sum \tilde{g}_i f_i + \tilde{h}) = \min\{in(\tilde{g}_i f_i); \; in(\tilde{g}_r f_r), in\, h\} = in(f)$ Also $inf = in \tilde{f}$ | $in(f - \tilde{f}) < in(f)$

Eigenschaften von Monomordnungen

1) $in(g \cdot f) = in(g) \cdot in(f)$

2) $in(g+f) \leq \min(in(g), in(f))$ und Gleichheit gilt, wenn $in(g) + in(f) \neq 0$

Ist $f - \tilde{f} = \sum_{i=1}^{r} g_i' f_i + h'$ dann ist $g_i = \tilde{g}_i + g'$, $h = \tilde{h} + h'$ die gesuchte Darstellung.

Eindeutig ist klar: Ist 2) erfüllt so haben $g_1 f_1, \dots, g_r f_r, h$ Leitterme mit verschiedenen Monomen.

Also $in(\sum g_i f_i + h) = \min\{in\, g_1 f_1, \dots, in\, g_r f_r, in(h)\}$

$$\Rightarrow in\, g_1 = 0 \quad in(h) = 0$$

$$\Rightarrow g_1, \dots, g_r, h = 0$$

Bemerkung: $g_1, \dots, g_r$ und h hängen von der Anordnung von $f_1, \dots, f_r$ ab, weil die Partition der Monome von der Anordnung abhängt.

11.4 Def. (vorl.) $f_1, \dots, f_r$ bilden eine Gröbnerbasis bzgl. $>$ falls der Rest ~~von~~ für jedes $f \in P$ der Rest h ~~bei~~ der Division mit $f_1, \dots, f_r$ nicht von der Reihenfolge von $f_1, \dots, f_r$ abhängt.

Sei $I \subset P$ ein Ideal, ~~Dann heißt~~ $>$ Monomordnung. Dann heißt

$$in(I) = \langle in(f) \mid f \in I \rangle$$ das Initialideal von I.

Elemente $f_1, \dots, f_r \in I$ nennt man eine Gröbnerbasis von I wenn $\langle in(f_1), \dots, in(f_r) \rangle = in(I)$ erzeugen.

~~Divisionssatz~~

$f_1, \dots, f_r \in K[x_1, \dots, x_n] = P$ globale Monomordnung $\forall f \in K[x_1, \dots, x_n]$

$\exists!\, g_1, \dots, g_r \in P$, $h \in P$, so dass

1) $f = g_1 f_1 + \dots + g_r f_r + h$

2) Kein Term von $g_i\, in(f_i)$ ist durch ein $in(f_j)$ mit $j < i$ teilbar.
Kein Term von h ist durch ein $in(f_i)$ teilbar

$f = \sum f_\alpha x^\alpha \quad in(f) = in(f) = f_\beta x^\beta$ wobei $\beta = \max\{\alpha \mid f_\alpha \neq 0\}$

~~Definition: $I \subset P$ Ideal $f_1, \dots, f_r$ von I~~

$$I : J = \{r \in R \mid r \cdot J \subset I\} \quad I, J \subset R \text{ Ideale}$$

Betrachten die Monomialen Ideale

$$M_i = \langle in(f_1), \dots, in(f_{i-1}) \rangle : in\, f_i \quad i = 2, \dots, r$$

$x^\alpha \in M_i \quad x^\alpha\, in(f_i) = c x^\beta\, in\, f_j \quad j < i$

$$S(f_i,f_j) = \frac{in(f_j)}{ggT(in(f_i),in(f_j))}\cdot f_i - \frac{in\, f_i}{ggT(in(f_i),in(f_j))} f_j$$

S-Polynom nach Buchberger

11.6 Satz (Buchbergers Kriterium)

$f_1,\dots,f_r \in \underline{P}$ bilden eine Gröbnerbasis von $\langle f_1,\dots,f_r\rangle$ genau dann wenn für jedes i und jeden Erzeuger x^α der Rest $x^\alpha f_1$ dividiert nach $f_1,\dots,f_n$ null ist

Buchbergers Formulierung

$\Leftrightarrow$ Für jedes Paar f_i, f_j der Rest bei Division $f_1,\dots,f_r$ von S-Polynom $S(f_i,f_j)$ null ist.

Beweis Die Notwendigkeit ist klar $in(I) = \langle in(f_1),\dots,in(f_r)\rangle$
$\Rightarrow$ Rest h von jedem $f\in I$ ist null. Dies ist hinreichend.
Für jedes Paar (i,α), $x^\alpha \in M$ haben wir eine Darstellung

$$x^\alpha f_i = \sum_{j=1}^{r} g_j^{(\alpha,i)} f_j \qquad P^r \longrightarrow P$$

$$e_i \longmapsto f_i$$

Dann ist $G(i\alpha) = (-g_1^{(i\alpha)},\dots, x^\alpha - g_i^{(i\alpha)},\dots,-g_r^{(i\alpha)}) \in \ker\varphi$ eine sog. Syzygie
Sei $f\in\langle f_1,\dots,f_r\rangle$ etwa $f = g_1f_1+\dots+g_rf_r$
Dann genügen $g_1,\dots,g_r$ den Bedingungen
2) im Divisionssatz, so $in(f) = \max\{in(g_i)\, in(f_i) \mid i=1,\dots,r\}$, da diese Terme zu disjunkten Monomen sind $\in \langle in(f_1),\dots,in(f_r)\rangle$

Monomordnungen lassen sich auch auf P^r mit Basis $e_1,\dots,e_r$, $e_j = (0\dots1\dots0)$ einführen.
Monome in P^r ist ein $x^\alpha e_j$ globale Monomordnung auf P^r ist vollständige Anordnung d. Monome so

a) $x^\alpha e_j > x^\beta e_i \Rightarrow x^\gamma x^\alpha e_j > x^\gamma x^\alpha e_i$

b) $x_i e_j > e_j$ (global) $i=1,\dots,n$ $j=1,\dots,r$

Divisionssatz in P^r $>$ globale Monomordnung auf P^r, $f_1,\dots,f_r\in P^r$ $\forall f\in P^r$

$\exists!\, g_1,\dots,g_n \in P\ \exists!\, h\in P^r$ sodass

1) $f = g_1f_1+\dots+g_rf_r+h$

2) Kein Term in $g_i\, in f_i$ ist durch ein $in f_j$ $j<i$ teilbar. Kein Term von h ist

ist durch $in(f_i)$ teilbar.

Def $f_1, \dots, f_r \in P^s$
$P^r \to P^s$
$e_i \mapsto f_i$

Sei $>$ eine globale Monomordnung auf P^s
Dann ist die induzierte Monomordnung auf P^r durch $x^\alpha e_i > x^\beta e_j \iff x^\alpha in(f_i) > x^\beta in(f_j)$ oder $x^\alpha in(f_i) = x^\beta in(f_j)$ und $i > j$

Lemma $in G^{(i,\alpha)} = x^\alpha e_i$

Beweis: Ein Term von $(-g_1^{(i,\alpha)}, \dots, g_r^{(i,\alpha)})$ hebt im Bild den Term $x^\alpha in(f_i)$ weg. Für diesen Term haben wir Gleichheit und $j < i$, also $x^\alpha e_i >$ dieser Term. Die ~~Terme in Differenz haben~~ Bilder aller anderen Terme $G^{(i,\alpha)}$ haben in P alle ~~kleiner~~ einen Leitterm, der kleiner als $x^\alpha in(f_i)$ ist also auch Terme sind bzgl. der induzierten Monomordnung ebenfalls kleiner als $x^\alpha e_i$ □

Sei $f = a_1 f_1 + \dots + a_r f_r \in I$
Betrachte $A = a_1 e_1 + \dots + a_r e_r \in P^r$ und dividieren A nach den $G^{(i,\alpha)}$. Den Rest H bei dieser Division
$$H = g_1 e_1 + \dots + g_r e_r$$
erfüllt die Bedingungen 2) Für die Koeffizienten $g_1, \dots, g_r$ bei Division nach $f_1, \dots, f_r \in P$
Es gilt: $f = a_1 f_1 + \dots + a_r f_r = g_1 f_1 + \dots + g_r f_r$ da die $G^{(i,\alpha)}$ Syzygien sind. Also $in(f) \in \langle in(f_1), \dots, in(f_r) \rangle$

Korollar $f_1, \dots, f_r$ GB in P^s
Sei $G^{(i,\alpha)}$ bilden eine Gröbnerbasis von $\ker(P^r \to P)$ bzgl. der Induzierten Ordnung. ~~Sei $G \in \ker f$~~

Beweis Sei $G \in \ker(P^r - P)$ beliebig und A der Rest von G bei der Division
$G = (g_1, \dots, g_r)$, $A = (a_1 e_1 + \dots + a_r e_r)$
Dann gilt: $a_1 f_1 + \dots + a_r f_r = g_1 f_1 + \dots + g_r f_r = 0$
$a_1 = 0, \dots, a_r = 0$ aus der Eindeutigkeit der Division nach $f_1, \dots, f_r$
$in(G) \in \langle in\, G^{(i,\alpha)} \mid (i,\alpha) \rangle$ □

Corollar (Hilbertsche Syzygiensatz)
$P = k[x_1, \dots, x_n]$ und M ein endlich erzeugtes P-Modul. Dann bes. M eine endliche freie Auflösung
$$0 \leftarrow M \leftarrow P^{r_0} \xleftarrow{\varphi_1} P^{r_1} \xleftarrow{\varphi_2} P^{r_2} \leftarrow \dots \leftarrow P^{r_n} \leftarrow 0$$
$\ker \varphi_i = \operatorname{Im} \varphi_{i+1} \quad i = 1, \dots, r$

Beweis: Wir können die Berechnung von Syzygien aus einer GB iterieren.

Sortiere $f_1, \dots, f_r$ so, dass der Exponent von x_n in $in(f_i)$ größer als der Exponent von x_n in $in(f_j)$ für ~~~~ $i > j$ gilt.
Dann taucht die Variable x_n in den M_i's nicht auf.
Im zweiten Schritt sortieren nach den Exponenten von x_{n-1} usw.
$\Rightarrow$ die Leitterme von Erzeugnis von ~~ker~~ Im φ_k involvieren nur die Variablen $(x_1, \dots, x_{n-k+1})$
Das Verfahren ~~berechnet~~ bricht nach spä teren n-Schritten ab.

Algorithmus zur Bestimmung von GB

Input $(f_1, \dots, f_r) \in P$,
Output GB   Durchlaufen aller Buchberger Test', wenn ein Rest $\neq 0$ nehmen wir $f_1, \dots, f_r$ hinzu und starten erneut.
Der Algorithmus terminiert mit einer GB, da jedes monomiale Ideal endlich erzeugt ist.

Algorithmus: Ideal membership

Input $f, f_1, \dots, f_r \in P$
Output Antwort auf $f \in \langle f_1, \dots, f_r \rangle$ + Darstellung $f = g_1 f_1 + \dots + g_r f_r$

1. Schritt Berechne eine GB von $\langle f_1, \dots, f_r \rangle$

2. Schritt: Berechne den Rest f dividiert nach $f_1, \dots, f_s$. Ist dieser Null, ist die Antwort ja und $f = g_1 f_1 + \dots + g_s f_s$. Ersetze anschließend die f_k mit $k > r$ durch Linearkombination von $f_1, \dots, f_{k-1}$ rekursiv und $f = \sum_{i=1}^{r} a_i f_i$ zu finden.

Corollar (Macaulay)

Sei $f_1, \dots, f_r$ eine GB. Dann repräsentieren die Monome $x^\alpha \notin \langle in(f_1), \dots, in(f_r) \rangle$ eine K-Vektorraumbasis von $P / \langle f_1, \dots, f_r \rangle$.