Algebra II

SS 05 gelesen von Prof. Dr. Bernd Siebert

Vorwort

Das ist meine Mitschrift zur Vorlesung “Algebra II” gelesen von Prof. Dr. Bernd Siebert an der Universität Freiburg im Sommersemester 2005.

Es besteht keine Garantie auf Richtigkeit und/oder Vollständigkeit. Ich möchte mich bei den Leuten bedanken, die mir dabei geholfen haben.

Falls ihr Fehler (jeder Art) findet, oder ein Kommentar oder sonts noch was habt, dann schreibt bitte an pabloy@pcpool.mathematik.uni-freiburg.de. Der LaTeX-Quellcode findet ihr unter http://pcpool.mathematik.uni-freiburg.de/~pabloy/alg2/. Der Code ist frei verfügbar und kann jeder Zeit heruntergeladen werden und verändert werden und anschließend eine Kopie weiter veröffentlicht werden. Die einzige Bedingung ist, dass man den Source Code weitergibt, sprich, dass meine Bedingung für alle erhalten bleibt.

Ich habe die Vorlesung “Algebra I” beim PD Dr. Jan-Christoph Schlage-Puchta während des Sommersemesters 2004 gehört. Damit aber eine gewisse Kompatibilität mit dem Stoff von der jetztigen Vorlesung gewährleistet wird, werde ich die Kapitel Nummerierung vom Prof. Dr. Bernd Siebert übernehmen.

Pablo Yánez Trujillo

Inhaltsverzeichnis

Abbildungsverzeichnis

Teil I

Einführung

Kapitel 22

Transzendente Körpererweiterungen

Ziel: Transzendensgrad (etwas wie eine Vektorraum Dimension)

22.1 Algebraische Abhängigkeiten

Definition
Sei L/K eine Körpererweiterung, $E \subset L$ heißt **algebraisch abhängig** *über K, wenn $a_1, \ldots, a_k \in E$, $k \geq 1$ existieren und $p \in K[x_1, \ldots, x_k] \setminus \{0\}$ mit $P(a_1, \ldots, a_k) = 0$. Ansonsten heißt E* **algebraisch unabhängig**.

22.2 Transzendenzerzeuger

Definition
Sei L/K Körpererweiterung, $E \subset L$ heißt **System von Transzendenzerzeugern** *über K, wenn $L/K(E)$ algebraisch ist.*

Bemerkung:

1. $E \subset L$ **maximal** (bezüglich Mengeninklusion) algebraisch unabhängige Teilmenge $\implies$ E ist ein System von Transzendenserzeugern.
2. $E \subset L$ minimales System von Transzendenzerzeugern $\implies$ E ist algebraisch unabhängig.

22.3 Transzendenzbasen

Definition
Eine **Transzendenzbasis** *ist ein algebraisch unabhängiges System von Transzendenzerzeugern.*

22.4 Austauschlemma

Lemma
Sei L/K eine Körpererweiterung und $E \subset L$ ein System von Transzendenzerzeugern. Dann gibt es für jede endliche, algebraische unabhängige Teilmenge $A \subset L$ ein $F \subset E$, $|F| = |A|$, so dass $(E \setminus F) \cup A$ System von Transzendenzerzeugern über K.

Beweis: Induktion nach $n = |A|$, $\quad n = 0$ (klar)

$n \longrightarrow n+1$ $A = \{a_0, \ldots, a_n\}$

IV. auf $A' = \{a_0, \ldots, a_{n-1}\}$ anwenden.

$\Longrightarrow$ $\exists\, F' \subset E$, $(E \setminus F') \cup A'$ System von Transzendenzerzeuger

$a_0 \in L \implies \exists\, p \in K[X_0, \ldots, X_n, Y_1, \ldots, Y_r]$, $b_1, \ldots, b_r \in E \setminus F'$, so dass $p(a_0, \ldots, a_n, b_1, \ldots, b_r) = 0$.

O.E.: Sei r minimal (A algebraisch unabhängig $\implies$ $r \geq 1$)

$$Q(y) := p(a_0, \ldots, a_n, y, b_2, \ldots, b_r) \in K(a_0, \ldots, a_n, b_2, \ldots, b_r)[Y]$$

Q hat Nullstellen in b_1, d.h. b_1 ist algebraisch über $K(a_0, \ldots, a_n, b_2, \ldots, b_r)$.

Setze $F := F' \cup \{b_1\}$ $\square$

Satz
Besitzt L/K ein endliches System von Transzendenzerzeugern über K, so hat L eine Transzendenzbasis über K. Je zwei solcher Transzendenzbasen haben gleich viele Elementen (endlich viele).

Beweis: Formal wie für Basen in der Linearen Algebra.

Definition 22.5

$$\mathrm{trdeg}_K L := \textit{Anzahl der Elemente einer Transzendenzbasis} \in \mathbb{N} \cup \{\infty\}$$

Beispiel: $\mathrm{trdeg}_K L(x_1, \ldots, x_k) = n$

Später: $\mathfrak{I} \subset K[X_1, \ldots, X_n] = R$ Primideal.

$$V(I) = \{x \in K^n \mid f(x) = 0 \ \forall\ f \in \mathfrak{I}\} \qquad \text{(algebraische Menge)}$$

Wir werden dann sehen: K abgeschlossen $\implies$ $\dim V(\mathfrak{I}) = \mathrm{trdeg}_L \mathrm{Quot}(R/\mathfrak{I})$.

Kapitel 0

Wiederholung elementarer Ringtheorie

0.1 Ringe

Definition Ringe
*Ein Ring (mit **Eins**) ist eine Menge R mit 2 inneren Verknüpfungen, geschrieben als Addition "+" und Multiplikation "$\cdot$", so dass folgende Bedingungen erfüllt sind:*

(a) R ist eine kommutative Gruppe bezüglich der Addition.

(b) R ist ein Monoid bezüglich der Multiplikation, d.h. die Multiplikation is assoziativ, und es existiert in R ein Einselement bezüglich der Multiplikation (muss nicht zwingend ein multiplikatives inverses Element für jedes Element von R geben).

(c) Es gelten die Distributivgesetze, d.h.

$$(a+b)\cdot c = a\cdot c + b\cdot c, \qquad c\cdot(a+b) = c\cdot a + c\cdot b), \qquad \text{für } a,b,c \in R$$

Bemerkung: "Mit Eins" bedeutet nicht die Zahl 1, sondern um das 1-Element, das multiplikativ neutrale Element eines Monoides(Gruppe)/Ringes.

Beispiele:

1. **Körper** $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_p = \mathbb{Z}/p, \mathbb{F}_{p^r} = \mathbb{F}_p[X]/(f)$, $\deg f = r$, f irreduzibel über $\mathbb{F}_p$
   $\mathbb{Q}(\alpha_1, \ldots, \alpha_r) \subset \mathbb{C}$, $\alpha_i \in \mathbb{C}$
   - $R/\mathfrak{m}$, R Ring, $\mathfrak{m}$ maximales Ideal. $\mathfrak{m}$ heißt maximal, wenn für alle Ideale $\mathfrak{a} \subset R$, für die gilt: $\mathfrak{m} \subset a \subset R \implies \mathfrak{a} = R$
   - Quot(R), R Integritätsbereich
2. **Polynomringe**: $K[T]$, $R[T]$, $K[T_1, \ldots, T_n] = (K[T_1, \ldots, T_{n-1}])[T_n] = K[\mathbb{N}^r]$
3. **Monoidringe**: $(M, +)$ Monoid, R Ring
$$R[M] = \left\{ \sum_{m \in M} a_m \chi^m \mid a_m \in R,\ a_m \neq 0 \text{ nur endlich oft} \right\}$$
4. **Faktorringe**: $R/\mathfrak{I}$, $\mathfrak{I} \subset R$, $\mathfrak{I}$ Ideal, etwa $\mathbb{C}[X,Y,Z]/(XY - Z^2)$

Im folgenden: Alle Ringe seien kommutativ mit Eins (1=0 möglich beim Nullring)

0.2 Ideale

Ideale: $\mathfrak{I} \subset R:\ \mathfrak{I}+\mathfrak{I} \subset \mathfrak{I},\ R\cdot\mathfrak{I} \subset \mathfrak{I}$

Bemerkung: Wenn $1 \in \mathfrak{I} \implies \mathfrak{I} = R$, ansonsten ist $\mathfrak{I}$ **nie** ein Ring.

Jede Teilmenge $S \subset R$ erzeugt ein Ideal

$$\mathfrak{s} = (S) = \{a_1 s_1 + \cdots + a_r s_r \mid a_i \in R,\ s_i \in S\}$$

Unsere Ringe haben die Eigenschaft, dass jedes Ideal **endlich erzeugt** ist, d.h. $\mathfrak{s} = (S),\ S$ endlich. (folgt aus der Eigenschaft "Noethersch" für Polynomringe: Hilbertscher Basissatz)

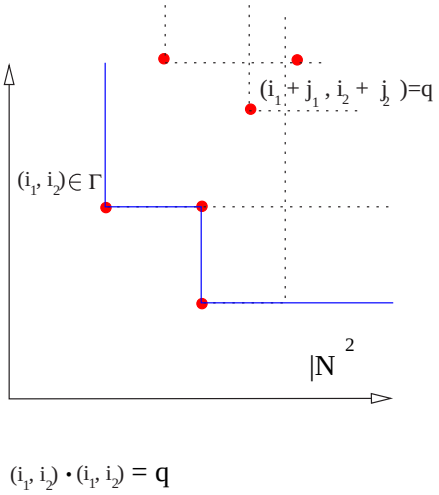

Abbildung 1: Menge von Exponenten in $\mathbb{N}^2$

Beispiele: 1. Sei $\Gamma \subset \mathbb{N}^r$ Menge von Exponenten. $\mathfrak{I} = \left(x_1^{i_1}, \ldots, x_r^{i_r}\right)_{(i_1,\ldots,i_r)\in\Gamma}$ ist endlich erzeugt gdw.

$$\left\{\gamma + \mathbb{R}^r_{\geq 0} \mid \gamma \in \Gamma\right\} \subset \mathbb{R}^r_{\geq 0}$$

hat endlich viele Ecken (Siehe Abbildung 1, die rote Punkte entlang der blauben Linie). Dies ist stets wahr (Beweis: später).

2. $R = K[\mathbb{Q}_{>0}]$. $\alpha_i \in \mathbb{Q},\ (\alpha_i)_{i\in\mathbb{N}}$ streng monoton fallend, $\mathfrak{I} = (\chi^{\alpha_i})$ **nie** endlich erzeugt.

Hauptideale: $\mathfrak{a}$ Ideal, $\mathfrak{a} = (a),\ a \in R$.

Hauptidealring: jedes Ideal eines solchen Ringes ist ein Hauptideal.

Beispiel: (eukdlidische Ringe) $\mathbb{Z}, K[T]$ aber i.a. **nicht** $R[T]$

0.3 Homomorphismen

Sei $\varphi : R \longrightarrow R$ ein Homomorphismus, dann gilt für alle $a, b \in R$:

- $\varphi(a+b) = \varphi(a) + \varphi(b)$
- $\varphi(a\cdot b) = \varphi(a)\cdot\varphi(b)$
- $\varphi(1) = 1$

$\mathrm{Kr}(\varphi) = \varphi^{-1}(0) \subset R$ ist ein Ideal.

$$R \twoheadrightarrow R/\mathrm{Kr}(\varphi) \xrightarrow{\overline{\varphi}} \mathrm{im}\varphi \hookrightarrow S$$

ist die kanonische Quotienten Abbildung.

Beispiel: $\varphi : R[T] \longrightarrow S \iff \varphi_0 : R \longrightarrow S,\ a \in S$

$\varphi \longmapsto (\varphi_0 = \varphi \restriction_R,\ a = \varphi(T))$

$\left(\sum \alpha_i T^i \longrightarrow \sum \varphi_0(\alpha_i)\alpha^i\right) \longleftarrow (\varphi_0, a)$

Sei $\varphi : R \longrightarrow S$ ein Homorphismus: Es gilt:

1. $R' \subset R$ Unterring $\implies$ $\varphi(R') \subset S$ Unterring
2. $S' \subset S$ Unterring $\implies$ $\varphi^{-1}(S') \subset R$ Unterring
3. $\mathfrak{I} \subset S$ Ideal $\implies$ $\varphi^{-1}(\mathfrak{I}) \subset R$ Ideal
4. $\mathfrak{I} \subset R$ Ideal $\overset{?}{\implies}$ $\varphi(\mathfrak{I}) \subset R$ Ideal

φ surjektiv.
Beispiel: $\varphi : K[X] \longrightarrow K[X,Y],\ X \longrightarrow X$.
$(x) = \{x \cdot f \mid f \in f[X]\},\ \varphi(x) = \{x \cdot f \mid f \in K[X]\} \subset K[X,Y]$ ist kein Ideal.
$\implies$ müssen i.a. das von $\varphi(\mathfrak{I}) \subset S$ erzeugte Ideal.

0.4 Algebren

Definition

(a) Sei R ein Ring. Eine R-Algebra ist ein Ring S zusammen mit einem Homomorphismus $R \longrightarrow S$.

(b) Eine R-Algebra S heißt **endlich erzeugt**, *wenn es $a_1, \ldots, a_k \in S$ gibt, so dass*

$$R[T_1, \ldots, T_k] \longrightarrow S,\ t_i \longrightarrow a_i$$

surjektiv ist.

Beispiel: S endlich erzeugte K-Algebra $\iff$ $S = K[T_1, \ldots, T_k]/\mathfrak{I}$

0.5 Primideale

Definition
$\mathfrak{p} \subset R$ *Primideal* $:\iff$ $(ab \in \mathfrak{p} \implies a \in \mathfrak{p}$ *oder* $b \in \mathfrak{p}) \iff R/\mathfrak{p}$ *ein Integritätsbereich ist.*

Beispiel:
1. $(n) \subset \mathbb{Z}$ Primideal $\iff$ n prim ist.
2. $\mathfrak{I} = (XY) \subset K[X,Y]$ ist **kein** Primideal $(XY \in \mathfrak{I}, X \notin \mathfrak{I},\ Y \notin \mathfrak{I})$
3. $(f) \subset K[X_1, \ldots, X_n]$ Primiedeal $\iff$ f unzerlegbar, gilt allgemein in faltoriellen Ringen
4. $\varphi : R \longrightarrow S,\ \mathfrak{p} \subset S$ Primideal $\implies$ $\varphi^{-1}(\mathfrak{p}) \subset R$ Primideal [Übung]

5. "Alles andere gilt i.a. nicht" $\mathfrak{p}_1 + \mathfrak{p}_2,\ \mathfrak{p}_1 \cap \mathfrak{p}_2, S \cdot \varphi(\mathfrak{p})$ keine Primideale

   - $\mathfrak{p}_1 = (x^2 + y^2 - z^2),\ \mathfrak{p}_2 = (z)$
     $\mathfrak{p}_1 + \mathfrak{p}_2 = (x^2 - y^2 - z^2, z) = (x^2 - y^2, z)$
     $(x+y) \cdot (x-y) \in \mathfrak{p}_1 + \mathfrak{p}_2$, aber $x + y, x - y \notin \mathfrak{p}_1 + \mathfrak{p}_2$
   - $\mathfrak{p}_1(X),\ \mathfrak{p}_2(Y) \subset K[X,Y]$
     $\mathfrak{p}_1 \cap \mathfrak{p}_2 = (XY),\ X \cdot Y \in \mathfrak{p}_1 \cap \mathfrak{p}_2,\ x \notin \mathfrak{p}_1 \cap \mathfrak{p}_2,\ y \notin \mathfrak{p}_1 \cap \mathfrak{p}_2$
   - $\varphi : K[T] \longrightarrow K[X,Y],\ T \longrightarrow XY$
     $\mathfrak{p} = (T),\ K[X,Y] \cdot \varphi(\mathfrak{p}) = (X \cdot Y)$ ist kein Primideal

6. Maximale Ideale sind Primideale.

0.6 Lokalisierung

$A \subset R$ multiplikativ abgeschlossen: $A \cdot A \subset A$

$A^{-1}R := R \times A/\sim$ mit $(a,b) \sim (a',b') \ :\Longleftrightarrow\ \exists\, c \in A :\ c(ab' - a'b) = 0$. Schreibweise: $[(a,b)] = a/b = \frac{a}{b}$

$A^{-1}R$ wird Ring vermöge $a/b + c/d := (ad + bc)/bd;\ (a/b) \cdot (c/d) := ac/bd$.

Es ist wohlefiniert: $a/b = a'/b' = a \cdot (ab' - b'a) = 0$ für ein $e \in A$.
$a'c/b'd \overset{!}{=} ac/bd \Longleftarrow e \cdot (a'cbd - acb'd) = cde(a'b - ab') = 0$

Speziellfälle:

1. R Integritätsbereich; $A := R \setminus \{0\},\ A^{-1}R = \mathrm{Quot}(R)$ Quotientenkörper.

2. A ist nicht abgeschlossen: ab Nullteiler $\implies \exists\, c \in R \setminus \{0\},\ abc = 0$ und es gilt
   $$\begin{cases} bc = 0 & \implies \quad b \text{ Nullteiler} \\ bc \neq 0 & \implies \quad a(bc) = 0, \text{ also } a \text{ ist Nullteiler} \end{cases}$$

   $\mathrm{Quot}(R) := A^{-1}R$ totler Quotientenring von R.
   Beispiel: $R = K[X,Y]/(X,Y),\ A = \{f \mid x \nmid f,\ y \nmid f\},\ \mathrm{Quot}(R) = \{(f_1/g_1, f_2/g_1) \in K[X,Y]\}$

   $g_1(0) \neq 0 \implies g_2(0) \neq 0$ und $\frac{f_1(0)}{g_1(0)} = \frac{f_2(0)}{g_2(0)}$.

   $\mathrm{Quot}(K[X,Y]/(XY)) \backsimeq K(X) \times K(Y),\ \frac{x+y}{x-y} \longrightarrow (1,-1) = (y = 0, x = 0)$

3. **Lokalisierung an einem Element**

   $f \in R,\ A := \langle f \rangle = \{f^n \mid n \in \mathbb{N}\},\ R_f := A^{-1}R$

   Diskussion: $R \longrightarrow R_f,\ a \longrightarrow a/1,\ \mathrm{Kr}(R \longrightarrow R_f) = \{a \in \mathbb{R} \mid \exists\, n : f^n a = 0\} =: \mathfrak{I}$
   [Übung: $R_q \backsimeq (R/\mathfrak{I})_f$]

   Insbesondere $R \longrightarrow R_f$ injektiv, gdw. f nicht Nullteiler ist. In diesem Fall $R_f \backsimeq R[T]/(Tf - 1)$

   Beweis: $\varphi : R[T] \longrightarrow R_f,\ T \longrightarrow 1/f$

   φ ist offensichtlich surjektiv, $aT^n \longrightarrow a/f^n,\ \mathrm{Kr}(\varphi) = (Tf - 1),\ g = b_0 + b_1 T + \cdots + b_r T^r \in \mathrm{Kr}(\varphi)$

$$\begin{array}{lll} \varphi \text{ nicht Nullteiler} & \iff & \frac{b_0}{1} + \frac{b_1}{f} + \cdots + \frac{b_r}{f^r} = 0 \text{ in } R \\ & \iff & 4 \text{ Nullstelle in } h = b_0U^r + b_1U^{r-1} + \cdots + b_r \in R[U] \\ & \overset{\text{Polynomdivision}}{\iff} & h = (U - f) \cdot h_1 \\ & \iff & U - fT \mid b_0U^r + b_1U^{r-1}T + \cdots + b_rT^r \\ & \iff & 1 - fT \mid g \\ & \iff & g \in (1 - fT) \end{array}$$

4. **Lokalisierung an einem Primideal $\mathfrak{p}$**

   $A = R \setminus \mathfrak{p}$ multiplikativ abgeschlossen. $R_\mathfrak{p} := A^{-1}R$ etwa $\mathfrak{p} = (x) \subset K[X]$, dann
   $K[X]_\mathfrak{p} = \left\{ \frac{f}{g} \mid XXg \right\} = \left\{ \frac{f}{g} \mid g(0) \neq 0 \right\}$

   Vorsicht: $K[X]_X \neq K[X]_{(X)}$, da $K[X]_X = (\langle x \rangle)^{-1}K[X]$ und $K[X]_{(X)} = ((K[X]/(X))^{-1}K[X]$.

0.7 Moduln

Ein Modul ist ein Vektorraum über einen Ring.

Definition R-Moduln
Ein R-Modul ist eine kommutative Gruppe $(M, +, \circ)$ zusammen mit einer Abbidldung $R \times M \longrightarrow M,\ (a, m) \longrightarrow (a \cdot m) = am$ mit folgenden Eigenschaften:

$$\begin{array}{rcl} \forall\ a, b \in R,\ \forall\ m, n \in M: & & \\ (a + b)m & = & am + bm \\ (ab)m & = & a(bm) \\ 1m & = & m \\ a(m + n) & = & am + an \end{array}$$

Erlaubt die Uniforme Behandlung folgender bekannter Speziallfälle.

1. $R = K,\ R-$Modul $= K = V \setminus R$.
2. $\mathfrak{I} \subset R,\ \mathfrak{I}$ Ideal ist ein R-Modul.
3. $R/\mathfrak{I}$ ist R-Modul.
4. $\varphi : R \longrightarrow S$ macht es zu R-Modul.
5. Abelsche Gruppe sind $\mathbb{Z}$-Module, $n \cdot g = \underbrace{g + \cdots + g}_{n}$
6. K-VR V mit $A \in \mathrm{End}(V)$ sind $K[X]$ Module.

Man definiert Untermoduln, Modulhomomorphismen und Quoteintenmoduln analog zu den entsprechenden VR-Begriffen.

Definition

(a) Ein R-Modul heißt **endlich erzeugt**, *gdw. $\exists\ a_1, \ldots, a_n \in M$ mit $M = Ra_1 + \cdots + Ra_n$*
[d.h. es existiert ein Epimorphismus (Surjektion) aus $R^n \longrightarrow M;\ e_i \longmapsto a_i$]

(b) Ein **zyklischer R-Modul** *wird von einem Element erzeugt.*
[$\Longrightarrow$ $M \simeq R/\mathfrak{I}$ vermöge $R \longrightarrow M,\ 1 \longmapsto a$, wobei a der Erzeuger ist]

0.8 Ausblick in die Kommutative Algebra und alg. Geometrie

Klasische Algebraische Geometrie

$\mathfrak{I} = (f_1, \ldots, f_r) \subset K[X_1, \ldots, X_n]$
$V(\mathfrak{I}) := \{x \in K^n \mid f(x) = 0; \quad \forall\ f \in \mathfrak{I}\} = V(f_1) \cup \cdots \cup V(f_r)$ ist eine **algebraische Menge**.

Wenn $K = \mathbb{C}$ oder irgendein abgeschlossener Körper, so liefert $\mathfrak{I} \longrightarrow V(\mathfrak{I})$ ein Lexikon kommutativer Algebra $\leftrightarrow$ Geometrie.

(Radikal-)Ideale $\subset R$	$\overset{1:1}{\leftrightarrow}$	algebraischer menge $\subset K^n$ [Hilbertscher Nullstellensatz]
Primideale	$\overset{1:1}{\leftrightarrow}$	unzerlegbarer algebraischen Menge* (=algebraische Varietät)
$R/\mathfrak{I}$	$\leftrightarrow$	algebraischen Funktionen auf $V(\mathfrak{I})$
$\mathrm{Quot}(R/\mathfrak{I})$	$\leftrightarrow$	rationalen Funktionen auf $V(\mathfrak{I})$
$h \in R,\ R_h$	$\leftrightarrow$	algebraischen Funktionen auf $K^n \setminus V(h) = \{x \in K^n \mid h(x) \neq 0\}$
maximale Ideake $\mathfrak{m} \subset \mathfrak{I}$ $(x_1 - a_a, \ldots, x_n - a_n)$	$\leftrightarrow$	$(a_1, \ldots, a_n) \in V(\mathfrak{I})$

* M algebraische Menge. M zerlegbar, gdw es existieren $A, B \subset M$, so dass gilt: $M = A \biguplus B$ und A, B algebraisch.

Moderner Standpunkt (ab ∼1960, Grothendieck 1958 - 1970)

Definition
*Sei R ein Ring. Das "***Spektrum***" von R ist definiert durch*

$$\mathrm{Spec}\ R := \{\mathfrak{p} \subset R \text{ Primideal}\}$$

Für beliebige Ringe R ersetze K^n durch das "Spektrum" von R^n versehen mit der **Zariski-Topologie**.

Benutze den geometrischen Fall $R = K[X_1, \ldots, X_n]/\mathfrak{I}$ als leitende Intuition; liefert auch neue Ergebnisse für diesen Fall.

Teil II

Kommutative Algebra

Kapitel 1

Monomenordnung

Monomenordnungen sind ein zentrales Hilfsmittel zur algorithmischen Behandlung von Polynomen in mehreren Veränderlichen.

Kovention: In $K[X_1, \ldots, X_n]$ schreibe $X^\alpha := X_1^{\alpha_1} \cdots X_n^{\alpha_n}$ für $\alpha = (\alpha_1, \ldots, \alpha_n)$ verträglich mit $K[\mathbb{N}^n] \simeq K[X_1, \ldots, X_n]$.

1.1 Ordnungen

Definition

(a) Eine **Teilordnung** *auf einer Menge M ist eine Relation $\leq$ für gewiesse Paare $(x, y) \in M \times M$ mit*

$$\begin{aligned} x \leq y,\ y \leq z &\implies x \leq z \\ x \leq y,\ y \leq x &\iff x = y. \end{aligned}$$

(b) Eine **Ordnung** *ist eine Teilordnung, die für alle Paaren definiert ist.*

(c) Eine **Wohlordnung** *ist eine Ordnung, bei der jede Teilmenge $S \subset M$ ein kleinstes Element besitzt, d.h. $\exists\ x \in S :\ \forall\ y \in S : x \leq y$.*

Beispiele:

1. Sei N eine Menge, $M = \mathfrak{P}(N),\ A, B \subset N,\ A \leq B \ :\iff\ A \subset B$ ist eine Teilordnung.
2. $(\mathbb{Z}, \leq)$ Ordung, keine Wohlordnung.
3. $(\mathbb{N}, \leq)$ Wohlordnung.
4. $M = \mathbb{N}^n,\ (\alpha_1, \ldots, \alpha_n) \leq (\beta_1, \ldots, \beta_n) \ :\iff\ \alpha_i \leq \beta_i \ \ \forall\ i$ ist eine Teilordnung. Die Bezeichnung für diese Relation ist: "$\leq_{\text{nat}}$"

Konvention: $x < y \ :\iff\ x \leq y,\ x \neq y$.

1.2 Monomordnung

Definition

Eine **Monomordnung** *auf $K[X_1, \ldots, X_n]$ ist eine Ordnung $\leq$ auf $\mathbb{N}^n$ mit der Eigenschaft:*

$$\alpha \leq \beta,\ \gamma \in \mathbb{N}^n \implies \alpha + \gamma \leq \beta + \gamma.$$

Bemerkung: Diese induzierte eine Ordnung auf den Monomen von $K[X_1, \ldots, X_n]$, $X^\alpha \leq X^\beta \iff \alpha \leq \beta$.

1.3 "Leit-"Begriffe

Definition
Sei $\leq$ eine Monomordnung und $f = a_{\alpha_1} X^{\alpha_1} + \cdots + a_{\alpha_d} X^{\alpha_d} \in K[X_1, \ldots, X_n]$ mit $\alpha_1 > \cdots > \alpha_d$. Wir nennen:

(a) $\mathrm{LM}(f) := X^{\alpha_1}$*:* **Leitmonom** *von f*

(b) $\mathrm{LE}(f) := \alpha_1$*:* **Leitexponent** *von f*

(c) $\mathrm{LT}(f) := a_{\alpha_1} X^{\alpha_1}$*:* **Leitterm** *von f*

(d) $\mathrm{LK}(f) := a_{\alpha_1}$*:* **Leitkoeffizient** *von f.*

1.4 Beispiele verschiedener Ordnungen

1. **(Reine) Lexikographische Ordnung (lex,lp)**

   $X^\alpha >_{\mathrm{lp}} X^\beta \iff \exists\, i : \alpha_1 = \beta_1, \ldots, \alpha_{i-1} = \beta_{i-1},\ \alpha_i > \beta_i$
   d.h. der erste Verschiedene Eintrag (von links) ist größer.

   Beispiel:

   (a) $XY^2 >_{\mathrm{lp}} Y^3Z^4$
   (b) $X^3Y^2Z^4 >_{\mathrm{lp}} X^3Y^2Z$

2. **Graduiert revers-lexikographische Ordnung (grevlex,dp)**

   $X^\alpha >_{\mathrm{dp}} X^\beta \iff \deg X^\alpha = \sum \alpha_i > \deg X^\beta = \sum \beta_i$ oder

   $\deg X^\alpha = \deg X^\beta$ und $\exists\, i : \alpha_i < \beta_i,\ \alpha_{i+1} = \beta_{i+1}, \ldots, \alpha_n = \beta_n$

   Beispiel:

   (a) $X^4Y^4Z^7 >_{\mathrm{dp}} X^5Y^5Z^4$, weil $4 + 4 + 7 > 5 + 5 + 4$
   (b) $XY^5Z^2 >_{\mathrm{dp}} X^4YZ^3$, weil $i = n$
   (c) $X^4YZ >_{\mathrm{dp}} X^3X^2Z$, weil $i = n - 1$

3. **Negative lexikographische Ordnung (neglex,ls)**

   $X^\alpha >_{\mathrm{ls}} X^\beta \iff X^\beta >_{\mathrm{lp}} X^\alpha$

   Beispiel:

   (a) $\forall\ \alpha \neq 0 : \quad 1 > X^\alpha$

1.5 Globale und lokale Ordnung

Definition
Eine Monomordnung $<$ heißt

- **global**, *falls* $\forall\ \alpha \neq 0,\ X^\alpha > 1$
- **lokal**, *falls* $\forall\ \alpha \neq 0,\ 1 > X^\alpha$
- **gemischt**, *falls sonst*

Beispiel: 1.4, a,b: globale; 1.4 c: lokal

1.6 Charakterisierung globaler Ordnung

Satz
Für eine Monomenordnung $>$ auf $K[X_1, \ldots, X_n]$ sind äquivalent:
(a) $>$ ist global$[\forall\ \alpha \neq 0,\ X^\alpha > 1]$

(b) $\forall\ i:\ X_i > 1$

(c) "$>$" ist Wohlordnung

(d) $\alpha >_{\text{nat}} \beta \implies X^\alpha > X^\beta$

Beweis: a) $\longrightarrow$ b): trivial

b) $\longrightarrow$ c): Sei $S \subset \mathbb{N}^n$. Zu zeigen: es existiert kleinstes Element bzgl $<$.

Nach dem Dicksons Lemma existiert ein $B \subset S$ endlich mit $S \subset B + \mathbb{N}^n$. Sei $\alpha \in B$ kleinstes Element [B endlich]. Dann gilt: $\forall\ \beta \in S\ \exists\ \gamma \in B$ mit $\beta \in \gamma + \mathbb{N}^n$ und $\beta \geq \gamma \geq \alpha$ und eine Ungleichung strikt, falls $\beta \neq \alpha$
c) $\longrightarrow$ d): Angenommen $\alpha >_{\text{nat}} \beta$ und $X^\alpha < X^\beta \implies \gamma := \alpha - \beta \in \mathbb{N}^r \setminus \{0\}$, und $X^\alpha < 1$
[wäre $X^\gamma > 1:\ X^\alpha = X^{\gamma+\beta} > X^\beta$ Widerspuch]

$S := \mathbb{N} \cdot \gamma \subset \mathbb{N}^r$ hat kein kleinstes Element, Widerspruch, da $1 > X^\gamma > X^{2\gamma} > \cdots$

d) $\longrightarrow$ a) $\forall\ \alpha \in \mathbb{N}^r \setminus \{0\} \implies X^4 > X^0 = 1$ □

1.7 Reduktion nach einer Monomordnung

(Auch Teilen mit Rest in $K[X_1, \ldots, X_n]$)

Definition
Sie $f = a_{\alpha_1} X^{\alpha_1} + \cdots + a_{\alpha_d} X^{\alpha_d} \in K[X_1, \ldots, X_n]$ *heißt* **reduziert** *bzgl.* $G \subset K[X_1, \ldots, X_n]$, *falls* $\forall\ g \in G : \mathrm{LM}(g) \nmid X^{\alpha_i},\ i = 1, \ldots, d$

Algorithmus (Divisionalgorithmus)
Sei $<$ eine globale Monomordnung.

Eingabe: $f \in K[X_1, \ldots, X_n]$, $g_1, \ldots, g_s \in K[X_1, \ldots, X_n]$

Ausgabe: $a_1, \ldots, a_s, r \in K[X_1, \ldots, X_n]$
$f = a_1 g_1 + \cdots + a_s g_s + r$ und r ist reduziert bezüglich $g_1, \ldots, g_s$.

Schritt 1: Falls $\mathrm{LT}(g_1) \mid \mathrm{LT}(f) \implies f = a_1' g_1 + h'$ mit $a_1' = \frac{\mathrm{LT}(f)}{\mathrm{LT}(g_1)}$

Falls $\mathrm{LT}(g_1) \mid \mathrm{LT}(h') \implies f = a_1'' g_1 + h''$ mit $a_1'' = a_1' + \frac{\mathrm{LT}(h')}{\mathrm{LT}(g_1)}$

Usw, liefert $f = a_1 g_1 + h$ und $\mathrm{LT}(g_1) \nmid \mathrm{LT}(h)$

Wiederhole diesen Schritt mit $g_2, \ldots, g_s$.

Ergebnis: $f = a_1 g_1 + \cdots + a_s g_s$, $\mathrm{LT}(g_i) \nmid \mathrm{LT}(r_i)\ \forall\ i$

Schritt 2: Wiederhole Schritt 1 mit $f_1 = r_1 - \mathrm{LT}(r_1)$ statt f
, $\implies f = a_1 g_1 + \cdots + a_s g_s + \mathrm{LT}(r_1) + r_2$ [andere a_i]

weiter mit $f_2 = r_2 - \mathrm{LT}(r_2)$ usw, also

$$f = a_1 g_1 + \cdots + a_s g_s + \underbrace{\mathrm{LT}(r_1) + \cdots + \mathrm{LT}(r_k)}_{=r}$$

f nach $g_1, \ldots, g_s$ reduzieren, $f = a_1 g_1 + \cdots + a_s g_s + \underbrace{\mathrm{LT}(r_1) + \cdots + \mathrm{LT}(r_k)}_{=r} + \underbrace{r_{k+1}}_{=0}$.

$\mathrm{LT}(r_1) > \mathrm{LT}(r_2) > \cdots$

Der Algorithmus bricht ab, da $>$ Wohlordnung.

Bemerkung: Das Ergbnis $a_1 g_1, \ldots, a_s g_s, r$ hängt von der Reihenfolge $g_1, \ldots, g_s$.

1.8 Beispiel einer Reduktion

$f = X^Y + XY^2 + Y^2$, $g_1 = XY - 1$, $g_2 = Y^2 - 1$, $<_{\mathrm{nat}}$ gegeben.

Schritt 1: [f durch $g1$ teilen]:

$$X^2Y + XY^2 = \underbrace{(X+Y)}_{=a_1}(XY-1) + \underbrace{X + Y + Y^2}_{=h}$$

[h durch g_2 teilen] schon OK, d.h. $r_1 = X + Y + Y^2$

[f_1 durch g_1 teilen] ok

[f_1 duch g_2 teilen] $Y^2 + Y = 1 \cdot (X^2 - 1) + \underbrace{Y + 1}_{=r_2}$

Resultat: $X^2Y + XY^2 + Y^2 = (X+Y)(XY-1) + 1 \cdot (Y^2 - 1) + X + Y + 1$

1.9 Monomiale Ideale

Definition
Ein Ideal $\mathfrak{I} \subset K[X_1, \ldots, X_n]$ *heißt* **monomial**, *falls* $S \subset \mathbb{N}^n$ *existiert mit* $\mathfrak{I} = (X^\alpha)_{\alpha \in S}$

Beispiel: $\mathfrak{I} \subset K[X_1, \ldots, X_n]$ beliebiges Ideal, so ist $(\mathrm{LM}(f))_{f \in S} = (\mathrm{LM}(\mathfrak{I}))$ monomial (hängt von der Relation $<$ ab).

Satz
Monomial Ideale in $K[X_1, \ldots, X_n]$ entsprechen in eindeutiger Weise Teilmengen $S \subset \mathbb{N}^n$ mit $\mathfrak{I} = S + \mathbb{N}^n$ vermöge

$$\mathfrak{I} \longmapsto (X^\alpha)_{\alpha \in S} = \left\{ \sum_{\alpha \in S} a_\alpha X^\alpha \right\}$$

Beweis: Klar!

$\mathfrak{I}$ monomial $\implies$ $\mathfrak{I} = (X^\alpha)$.
$X^\alpha \in \mathfrak{I} \implies \forall\, \beta \in \mathbb{N}^n :\ X^{\alpha+\beta} \in \mathfrak{I}$, d.h. $(X^\alpha)_{\alpha \in S} = (X^\alpha)_{\alpha \in S' + \mathbb{N}^n}$, $\qquad S := S' = \mathbb{N}^n$

1.10 Idee für den Hilbertschen Satz

Ersetze $\mathfrak{I}$ durch $(\mathrm{LM}(\mathfrak{I})) = (X^\alpha)_{\alpha \in \mathrm{LE}(\mathfrak{I})}$ und zeige $\mathrm{LE}(\mathfrak{I}) \subset \mathbb{N}^n$ "endlich erzeugt", d.h. ex existiert ein $B \subset \mathrm{LE}(\mathfrak{I})$ endlich mit $\mathrm{LE}(\mathfrak{I}) = B + \mathbb{N}^n$.

Lemma (Dicksons Lemma)
Für $S \subset \mathbb{N}^n$ existiert eine endliche Menge $B \subset S$ mit $S \subset B + \mathbb{N}^n$. B ist ein erzeugendes System.

Mit anderen Worten: $\forall\, \alpha \in S\ \exists\, \beta \in B :\ \beta \leq_{\mathrm{nat}} \alpha$

Beweis: Induktion nach n $\qquad (S \neq \emptyset)$

$\underline{n = 1}$
$\alpha : 0 \min S,\ B = \{\alpha\}$

$\underline{n - 1 \longmapsto n}$
Betrachte die Projektion auf der $n-1$. ersten Koordinate
$Pr_n : \mathbb{N}^n \longrightarrow \mathbb{N}^{n-1}$, $(\alpha_1, \ldots, \alpha_n) \longmapsto (\alpha_1, \ldots, \alpha_{n-1})$.
$M_i := Pr_n(S \cap (\mathbb{N}^{n-1} \times \{i\}))$ $n-i$. Schicht.

Induktion Vor. $\implies$ $\exists\ B_i \subset M_i \subset \mathbb{N}^{n-1}$ endlich erzeugtes System. Weiter betrachte die Vereinigung $\bigcup_{i=0}^{s} B_i \times \{i\}$.

Zu zeigen: B ist Erzeugendessystem von S, $S \subset B + \mathbb{N}^{\cdot}$, $\alpha = (\alpha', j) \sin S$.

$\alpha' \in M_j \subset B_j + \mathbb{N}^{n-1}$

$\alpha' \in \gamma + \mathbb{N}^{n-1}$ für ein $\gamma \in B_j$.

Fall 1: $j \leq s \implies (\alpha', j) \in (\gamma, j) + \mathbb{N}^{n-1} \times \{0\} \subset B + \mathbb{N}^n$

Fall 2: $j > s \implies \exists\, \gamma' \in B' \cap B_i,\ i \leq s$ mit $\alpha' \in \gamma' + \mathbb{N}^{n-1}$, also
$(\alpha', j) \in (\gamma', i) + (\mathbb{N}^{n-1} \times \{j - i\}) \subset B + \mathbb{N}^n$ □

1.11 Hilberter Basissatz

Satz (Hilberter Basissatz)
Jedes Ideal $\mathfrak{I} \subset K[X_1, \ldots, X_n]$ ist endlich erzeugt.

Beweis: Sei $<$ eine lexikopgraphische Ordnung. Nach dem Dicksons Lemma existieren $g_1, \ldots, g_s \in \mathfrak{I}$ mit $\{\mathrm{LE}(g_1), \ldots, \mathrm{LE}(g_s)\} + \mathbb{N}^n = \mathrm{LE}(\mathfrak{I}) \implies (\mathrm{LM}(g_1), \ldots, \mathrm{LM}(g_s)) = (\mathrm{LM}(\mathfrak{I}))$

Dann gilt $\mathfrak{I} = (g_1, \ldots, g_s)$:

$f \in \mathfrak{I}$: Nach Division existieren $a_1, \ldots, a_s, r,\ f = a_1 g_1 + \cdots + a_s g_s + r$ und $\mathrm{LM}(g_i)$ teilt kein monom von r für $i \in \{1, \ldots, s\}$.

Aber $r = f - a_1 g_1 - \cdots - a_s g_s \in \mathfrak{I}$. Wäre $r \neq 0$, dann $\mathrm{LM}/r) \in (\mathrm{LM}(\mathfrak{I})) = (\mathrm{LM}(g_1), \ldots, \mathrm{LM}(g_s))$ (Widerspruch)

$\implies r = 0$

Bemerkung: Das letzte Argument im Beweis zeigt auch, dass $\mathfrak{G} \subset \mathfrak{I}$ das Ideal erzeugt, falls $(\mathrm{LM}(\mathfrak{G})) = (\mathrm{LM}(\mathfrak{I})) \iff \mathrm{LE}(\mathfrak{I}) \subset \mathrm{LE}(\mathfrak{G}) + \mathbb{N}^n$.

[Diese Eigenschaft hängt von der Ordnung $<$ ab].

1.12 Standard-Gröbner-Basen

Definition
Sei $<$ eine Monomordnung und $\mathfrak{I} \subset K[X_1, \ldots, X_n]$. $G = \{g_1, \ldots, g_s\} \subset \mathfrak{I}$ heißt **Standardbasis** *für $\mathfrak{I}$, falls* $\mathrm{LE}(\mathfrak{I}) < \mathrm{LE}(G) + \mathbb{N}^n$

Ist $<$ global, so redet man auch von den **Gröbnerbasen**.

Existenz: aus dem Beweis des Hilbertschen Satzes
Eindeutigkeit: Ja für reduzierte Standardbasen, d.h. g_i reduziert bzgl. $G \setminus \{g_i\}\ \forall\ i$

Bemerkung: Diese bestimmung einer Standardbasis ist **nicht** offensichtlich.

Beispiel: $\mathfrak{I} = (X^3 - 2XY, X^2Y + X - 2X^2)$
Standardbasis bzgl. $<_{\mathrm{lp}}$ $X^3;\ X - 2Y^2$
$<_{\mathrm{dp}}$ $2Y^2 - X;\ XY;\ X^2$
$<_{\mathrm{ls}}$ $2Y^2 - X - XY;\ 2XY - X^3;\ X^2$

1.13 Anwendung - Ideal Test

Der Beweis des Hilbertschen Satzes zeigt auch:

Satz
Sei $G = \{g_1, \ldots, g_s\}$ Standardbasis bzgl $<$. Für $\mathfrak{I} \subset K[X_1, \ldots, X_n],\ f \in K[X_1, \ldots, X_n]$ und $f = a_1 g_1 + \cdots + a_s g_s + r$ die Reduktion von f nach $g_1, \ldots, g_s$ gilt:

$$f \in \mathfrak{I} \iff r = 0$$

Bemerkung: Falls G nur $\mathfrak{I}$ erzeugt, ist dies i.a. nicht richtig.

1.14 S-Polynome

Wann ist $\{g_1, \ldots, g_s\}$ Standardbasis für $(g_1, \ldots, g_s)$? Antwort: 1.15

Problem: Für $p, q \in K[X_1, \ldots, X_n]$ undi, j lässt sich $\mathrm{LT}(pg_i - qg_j)$ schwer kontrollieren. Natürliche Kandidaten: $S(g_i, g_j)$.

Definition
Sei $<$ eine Monomordnung auf $K[X_1, \ldots, X_n]$ und $f, g \in K[X_1, \ldots . X_n]$.

S-Polynome *von f, g:*

$$S(f,g) := \frac{X^\gamma}{\mathrm{LT}(f)} \cdot f - \frac{X^\gamma}{\mathrm{LT}(g)} \cdot g$$

mit $\gamma := (\max\{\alpha_1, \beta_1\}, \ldots, \max\{\alpha_s, \beta_n\})\,,\ \alpha = \mathrm{LE}(f),\ \beta = \mathrm{LE}(g).$

Beispiel: $S(XY-1, Y^2-1) = \frac{XY^2}{XY}(XY-1) - \frac{XY^2}{Y}(Y^2-1) = (XY^2 - Y) - (XY^2 - X) = X - Y.$

1.15 Buchbergers Kriterium

Satz (Buchbergers Kriterium)
Sei $<$ eine Monomordnung auf $K[X_1, \ldots, X_n]$, $G = \{g_1, \ldots, g_s\}$ ist eine Standardbasis für (G) gdw, $\forall\, i, j:\ \mathrm{LM}(S(g_i, g_j)) \in (\mathrm{LM}(g_1), \mathrm{LM}(g_2))$.

Beweis: " $\Longrightarrow$ " $S(g_i, g_j) \in (G)$, benutze Definition von den Standardbasen.

"$\Longleftarrow$" 1.17 für globale Monomordnungen.

1.16 Lemma

Lemma
Seien $a_i \in K,\ f_i \in K[X-1, \ldots, X_n],\ \mathrm{LE}(f_i) = \delta \in \mathbb{N}^n$ über $<$ ($<$ Monomordnung),
$(*)$ $\mathrm{LE}(\sum a_i f_i) < \delta$. Dann gilt:

$$\forall\, i, j\ \mathrm{LE}(S(f_i, f_j))$$

(ACHTUNG: NICHT VOLLSTÄNDIG, ICH VERSTEHE AN DIESER STELLE MEINER AUFZEICHNUNGEN NICHT.)

Beweis: o.E. $\mathrm{LK}(f_i) = 1$

$S(f_i, f_j) = \frac{X^\delta}{X^\delta} f_i - \frac{X^\delta}{X^\delta} f_j = f_i - f_j$ hat LK $< \delta$

$$\begin{aligned} \textstyle\sum a_i f_i &= a_1(f_1 - f_2) + (a_1 + a_2)(f_2 - f_3) \\ &+ (a_1 + a_2 + a_3)(f_3 - f_4) + \cdots + (a_1 + \cdots + a_{5-1})(f_{5-1} - f_5) \\ &+ \underbrace{(a_1 + \cdots + a_5)}_{=0} f_5 \end{aligned}$$

$(*) \implies a_1 S(f_1, f_2) + (a_1 + a_2) S(f_2, f_3) + \cdots + (a_1 + \cdots + a_{5-1}) S(f_{5-1} - f_5)$ $\square$

1.17 Beweis von 1.15

Beweis: "$\Longleftarrow$": z.z. $f \in (g_1, \ldots, g_2) \implies \mathrm{LM}(f) \in (\mathrm{LM}(g_1), \ldots, \mathrm{LM}(g_s))$
sofern $\mathrm{LM}(S(g_i, g_j)) \in (\mathrm{LM}(g_1), \ldots, \mathrm{LM}(g_s))$.

Schreibe $f = \sum_{i=1}^{s} h_i g_i$ mit $\delta := \max\{\mathrm{LE}(h_i, g_i)\}$ minimal bzgl. aller solcher Darstellungen und behaupte
$(*)$ $\delta = \mathrm{LE}(f)$

Falls dies korrekt ist, dann existiert ein i mit $\mathrm{LE}(f) = \mathrm{LE}(h_i, g_i) = \mathrm{LE}(h_i) + \mathrm{LE}(h_i)$
$\mathrm{LM}(f) = \mathrm{LM}(h_i g_i) \in (\mathrm{LM}(g_i))$ fertig!

Beweis von $(*)$:

Angenommen $\delta > \mathrm{LE}(f)$.

Wir produzieren Darstellungen $f = \sum \hat{h}_i \hat{g}_i$ mit $\mathrm{LE}(\hat{h}_i, g_i) < \delta \ \forall\ i$ und das ist ein Widerspruch!

$\delta_{ij} := \mathrm{LE}(h_i g_j),\ \mathrm{LT}(h_i) a_i X^{\gamma_i}$

Schriebe

$$\sum h_i g_i = \sum_{\delta_i = \delta} \mathrm{LT}(h_i) g_i \quad + \underbrace{\sum_{\delta_j = \delta} (h_i - \mathrm{LT}(h_i)) g_i}_{< \delta} + \underbrace{\sum_{\delta_i = \delta} h_i g_i}_{< \delta}$$

$\mathrm{LE}(f) < \delta \implies \mathrm{LE}(\sum_{\delta_i = \delta} a_i X^{\gamma_i}) < \delta$

$\overset{\text{Lemma } 1.16}{\Longrightarrow} \sum a_i X^{\gamma_i} g_i \in (S(X^{\gamma_i} g_i, X^{\gamma_j} g_j))$.

$$S(X^{\gamma_i} g_i, X^{\gamma_j} g_j) = \frac{X^{\delta}}{X^{\gamma_i} \mathrm{LT}(g_i)} X^{\gamma_i} g_i - \frac{x^{\gamma}}{X^{\gamma_i} \mathrm{LT}(g_i)} X^{\gamma_j} g_j = X^{\delta - \gamma_{ij}} S(g_i, g_j)$$

mit $\gamma_{ij} = kgV\ \{\mathrm{LM}(g_i), \mathrm{LM}(g_j)\}$

$\implies \sum_{\delta_i = \delta} \mathrm{LT}(h_i) g_i \in \left(X^{\delta - \gamma_{jk}} S(g_j, g_k)\right) \subset (g_1, \ldots, g_s)$

$\overset{\text{Div. Alg.}}{\Longrightarrow} \exists\ q_{j,k} : \sum_{\delta_i = \delta} \mathrm{LT}(h_i) g_i = \sum_{j,k} q_{j,k} S(g_j, g_k)$

$\implies \exists\ p_{ijk} : \ a_{jk} S(g_s, g_k) = \sum_i p_{ijk} g_i$

div. Alg. zeigt: wir können erreichen: $\mathrm{LE}(p_{ijk}, g_i) < \delta$.

Setze $\hat{h}_i := \begin{cases} h_i & : \ \delta_i < \delta \\ \sum_{j,k} p_{ijk} + (h_i - \mathrm{LT}(h_i)) & : \ \delta_i = \delta \end{cases}$

Dann $f = \sum \hat{h}_i g_i$ wegen $(*)$ $\square$

1.18 Beispiel

Beispiel: $G = \{X - Z^2, Y - Z^3\}$ ist Gröbner-Basis von $(X - Z^2, Y - Z^3)$ bzgl. $<_{\text{lp}}$

Was ist $S(X - Z^2, Y - Z^3) = Y \cdot (X - Z^2) - X \cdot (Y - Z^3) = -YZ^2 + XZ^3$ reduzieren nach $X - Z^2, Y - Z^3$: $-YZ^2 + XZ^3 = Z^3(X - Z^2) + (-Z^2)(Y - Z^3) + 0$

1.19 Buchberger-Algorithmus

Algorithmus (Buchberger-Algorithmus)
Sei $<$ eine globale Ordnung:

Eingabe: $f_1, \ldots, f_s \in K[X_1, \ldots, X_n]$

Ausgabe: $g_1, \ldots, g_s \in K[X_1, \ldots, X_n]$ Gröbner-Basis bzgl. $<$ für $(f_1, \ldots, f_r)$.

Start: $g_1 = f_1, \ldots, g_r = f_r, \quad s = r$

Überprüfe Gröber-Kriterium:
$\forall\ i, j: \quad \mathrm{LE}(S(g_i, g_j)) \in \{\mathrm{LE}(g_1), \ldots, \mathrm{LE}(g_s)\} + \mathbb{N}^n$

Falls nein, $s \rightsquigarrow s + 1, \quad g_{s+1} := S(g_i, g_j)$ für (i, j) die $(*)$ verletzen.
Weiter mit $(*)$

Falls ja, fertig nach 1.15!

Der Algroithmus bricht ab, denn $S_i \subset \mathbb{N}^n$ ist die Menge der Leitexponente aus dem i-ten Schritt, so hat $\bigcup(S_i + N^r)$ ein endliches erzeugendes System $\subset S_1 \cup \cdots \cup S_a$ nach dem Dicksons Lemma.

"Nur" a Durchläufe sind nötig (nicht effizient, weil a sehr groß sein kann, auch wenn die Polynome einfach sind/aussehen).

[benutzt: $<$ ist Verfeinerung von $<_{\text{nat}}$, d.h. das gilt nur für globale Ordnung].

1.20 Beispiel

Beispiel: $f_1 = X^{10} + YZ, \ f_2 = Z^{10} + XY$ (Gröbner-Basis für $<_{\text{dp}}$)

$$\begin{array}{ll} \text{Gröbner} - \text{Basis} & <_{\text{lp}} \\ & \begin{array}{l} X^{11}Z + Z^{100} \\ XY + Z^{10} \\ XZ^{90} - Y^{10}Z \\ X^2Z^{80} - Y^9Z \\ X^3Z^{70} - Y^8Z \\ \qquad \vdots \\ X^{10} + YZ \end{array} \end{array}$$

Kapitel 2

Algebraische Mengen

Sei K ein beliebiger Körper (später algebraisch abgeschlossen)

2.1 Definition

Definition (Algebraische Mengen)
Für $S \subset K[X_1, \ldots, X_n]$ heißt

$$V(S) := \{a \in K^n \mid f(a) = 0, \ \forall \ \in S\}$$

(gemeinsame) **Nullstellenmenge** *von S.*

(V "Varietät") Teilmengen in K^n dieser Form heißen **algebraische Mengen**.

(a) **Hyperfläche** $V(f), \ f \in K[X_1, \ldots, X_n] \setminus \{0\}$

(b) $V(S) = V((S))$, *also reicht es für S Ideale zu betrachten*

(c) Hilberster Basissatz: $\exists \ f_1, \ldots, f_r \in K[X_1, \ldots, X_n], \ (S) = (f_1, \ldots, f_r)$

$$\implies \ V(S) = V(f_1, \ldots, f_r) = V(f_1) \cap \cdots \cap V(f_r)$$

(d) $A \subset K^1$ *algebraich* $\iff$ $A = K^1$ *oder A endlich.*

2.2 Eigenschaften algebraischer Mengen

Satz (Eigenschaften algebraischer Mengen)

(a) $\mathfrak{I} \subset \mathfrak{J} \implies V(\mathfrak{I}) \supset V(\mathfrak{J})$

(b) $\emptyset, \mathfrak{K}^n \subset K^n$ sind algebraisch

(c) $\{a\} \subset K^n$ ist algebraisch

(d) $V(\mathfrak{I}\mathfrak{J}) = V(\mathfrak{I} \cap \mathfrak{J}) = V(\mathfrak{I}) \cup V(\mathfrak{J})$

(e) $V(\sum \mathfrak{I}_r) = \bigcap V(\mathfrak{I}_r)$

Beweis:

(a) klar

(b) $\emptyset = V(1),\ K^n = V(0)$

(c) $V(X_1 - a_1, \ldots, X_n - a_n) = (a_1, \ldots, a_n)$

(d) $\mathfrak{I}\mathfrak{J} \subset \mathfrak{I} \cap \mathfrak{J},\ \mathfrak{J}$
(a) $\implies V(\mathfrak{I}\mathfrak{J}) \subset V(\mathfrak{I} \cap \mathfrak{J}) \supset V(\mathfrak{I}) \cup V(\mathfrak{J})$. Umgekehrt: $a \notin V(\mathfrak{I}) \cup V(\mathfrak{J})$

$\implies \exists\ f \in \mathfrak{I},\ g \in \mathfrak{J},\ f(a) \neq 0,\ g(a) \neq 0$

$\implies (fg)(a) \neq 0 \implies a \notin V(\mathfrak{I}\mathfrak{J})$

(e) $a \in V(\sum \mathfrak{I}_r) \iff \forall\ s \forall\ f_r \in \mathfrak{I}_{r_1}, \ldots, f_{r_s} \in \mathfrak{I}_{r_s}$
$f_{r_1}(a) + \cdots + f_{r_s}(a) = 0 \iff f \in \bigcap V(\mathfrak{I}_r)$

Bemerkung: Die $V(\mathfrak{I})$ bilden daher die abgschlossenen Mengen einer Topologie, der **Zariski-Topologie** auf K^n.

2.3 Abstrakte topologische Räume

Definition (Topologie)
Eine **Topologie** *auf einer Menge M ist ein System T von Teilmengen von M ($T \subset \mathfrak{P}(M)$) mit den folgenden Eigenschaften:*

(a) $\in T,\ M \in T$

(b) $\forall\ U, V \in T \implies U \cap V \in T$

(c) $U_\nu \in T \implies \bigcup U_\nu \in T$

Die so ausgezeichneten Teilmengen von M heißen **offen**, *ihre Komplemnete* **abgeschlossen**.

Topologischer Raum := Menge + Topologie

2.3.1 Beispiel

Beispiel:

1. Die triviale Topologie $T = \{\emptyset, M\}$
2. Die diskrete Topologie $T = \mathfrak{P}(M)$
3. d Metrik auf M, so sei $U \subset M$ offen $:\iff \forall\ P \in U\ \exists\ \varepsilon > 0 :\ B_\varepsilon(P) \subset U$.

   Solche Räume heißen metrisierbar.
4. $M = \{0, \eta\},\ T = \{\emptyset, M, \{\eta\}\}$

   Auch Punkte (Einpunktige Mengen) können offen sein.

5. $M = \mathbb{R}$ Zariski-Topologie

$$\emptyset \subset U \subset M \text{ offen} \iff U = M \setminus \text{endliche Menge}$$

2.3.2 Interpretation

Eine Topologie verleiht eine Menge "Gestalt", z.B. $\mathbb{R}$ und $S^1 \subset \mathbb{R}^2$ sind als Mengen "gleich" (es existiert eine Bijektion) als Topologische Räume (mit den metrischen Topologien) aber grundverschieden (S^1 kompakt, $\mathbb{R}$ nicht).

2.4 Existenz von Nullstellen im alg. absch. Fall

Falls K nicht algebraisch abgeschlossen, so kann $V(\mathfrak{I}) = \emptyset$ sein, obwohl $\mathfrak{I} \neq K[X_1, \ldots, X_n]$:
$K = \mathbb{R},\ n = 1,\ \mathfrak{I} = (x^2 + 1)$.

Satz (Hilbertscher Nullstellensatz, schwache Form)
Ist K algebraisch abgeschlossen und $\mathfrak{I} \subset K[X_1, \ldots, X_n],\ \mathfrak{I}$ ideal, dann $V(\mathfrak{I}) \neq 0$

Beweis: Es existiert ein maximales Ideal $\mathfrak{m} \subset K[X_1, \ldots, X_n]$ mit $\mathfrak{I} \subset \mathfrak{m}$ (Satz 2.7)

$L := K[X_1, \ldots, X_n]/\mathfrak{m}$ ist Körpererweiterung von K, die endlich erzeugt ist als K-Algebra
[d.h. $\exists\ K[X_1, \ldots, X_n] \twoheadrightarrow L$].

Satz 2.5 $\implies$ L/K algebraisch.

K algebraisch abgeschlossen $\implies$ $L = K$. Betrachte $\varphi : K[X_1, \ldots, X_n] \xrightarrow{/\mathfrak{m}} L = K,\ x_i \longmapsto a_i$.

Dann $(a_1, \ldots, a_s) \in V(\mathfrak{I})$: $f \in \mathfrak{I} \implies f \in \mathfrak{m} = \mathrm{Kr}\varphi \implies f(a_1, \ldots, a_m) = \varphi(f) = 0 \implies f \in V(\mathfrak{I})$ $\square$.

2.5 Lemma (Aus der Körpertheorie)

Lemma
Sei L/K Körpererweiterung und L endlich erzeugt als K-Algebra. Dann ist L/K eindlicher algebraischer Körper.

Beweis: allgemeiner Fall: später (ganze Ringerweiterungen)

Für K überabzählbar [etwa für $\mathbb{C} \subset K$, aber etwa nicht für den algebraischen Abschluss von $\mathbb{Q}$].

$L = K[\alpha_1, \ldots, \alpha_n]$ hat abzählbares Erzeugendessystem als K-UR. Wäre $x \in L$ transzendent, dann wäre $\frac{1}{x-\beta},\ \beta \in K$ überabzählbares System K-lin. unabhäniger Elemente von L $\square$.

2.6 Existenz maximaler Ideale I

Die Existenz maximaler Ideale beruhrt auf das Lemma von Zorn. Sei $(M,\ <)$ eine teilgeordnete menge und jede (total) geordnete Teilmenge $S \subset M$ hat eine obere Schranke in M $(x \in M,\ \forall\ y \in S,\ y < x)$.

Das folgt aus dem Auswahlauxion.

2.7 Existenz maximaler Ideale II

Satz
Sei R ein Ring, $\mathfrak{I} \subset R$ echtes Ideal, dann existiert $\mathfrak{m} \subset R$ maximales Ideal mit $\mathfrak{I} \subset \mathfrak{m}$.

Index