

15. Vorlesung, 1.12.2010

2.4.18 Satz Sei R Integritätsring, $x_1, \dots, x_n \in R$.

- (i) Falls $(x_1, \dots, x_n) = (d)$ für ein $d \in R$, so $d = \text{ggT}(x_1, \dots, x_n)$.
- (ii) Falls $(x_1) \cap \dots \cap (x_n) = (v)$ für ein $v \in R$, so $v = \text{kgV}(x_1, \dots, x_n)$.

Beweis (i) $\forall i: x_i \in (d) \Rightarrow d \mid x_i; d \in (x_1, \dots, x_n) \Rightarrow d = a_1 x_1 + \dots + a_n x_n$
 Also $\forall i: d' \mid x_i \Rightarrow d' \mid d$. (ii) analog $\square$

2.4.19 Satz (Euklidischer Algorithmus)

Sei (R, δ) ein euklidischer Ring, $a, b \in R \setminus \{0\}$

Betrachte die Folge $r_0 = a, r_1 = b, r_{i+1} = \text{Rest von } r_{i-1} \text{ bei Division durch } r_i$, falls $r_i \neq 0$, 0 sonst.

Dann gibt es einen kleinsten Index $n \in \mathbb{N}$ mit $r_{n+1} = 0$
 und gilt $r_n = \text{ggT}(a, b)$:

$$a = b q_1 + r_2, \quad \delta(r_2) < \delta(b) = \delta(r_1)$$

$$b = r_2 q_2 + r_3, \quad \delta(r_3) < \delta(r_2)$$

$$r_2 = r_3 q_3 + r_4, \quad \delta(r_4) < \delta(r_3)$$

$\vdots$

$$r_{n-2} = r_{n-1} q_{n-1} + r_n, \quad \delta(r_n) < \delta(r_{n-1})$$

$$r_{n-1} = r_n q_n.$$

2.4.20 Ausblick auf der algebraischen Geometrie

Die alg. Geom. studiert die geom. Eig. der algebraischen Teilmengen (d.h. Nullstellen von Polynomen) mit Hilfe der alg. Eig. der assoziierten Ideale, Ringen, Körper usw.

Sei $K = \mathbb{C}$ oder ein algebraisch abgeschlossener Körper.

Eine Teilmenge $Y \subset K^n$ heißt (affin)-algebraisch, falls $\exists T \subset K[X_1, \dots, X_n]$ mit $Y = Z(T) := \{z \in K^n: \forall P \in T, P(z) = 0\}$.

Z.B. $\{(z, w) \in K^2 : w = z^2\}$, $\{(z, w) \in K^2 : zw = 0\}$,
 alg. Teilmengen in $\mathbb{C}$ sind endliche Teilmenge von $\mathbb{C}$.

Endliche Vereinigung und bel. Durchschnitt von alg. Teilmengen
 sind alg. Teilmengen.

Eine alg. Teilmenge heißt *irred.* falls aus $Y = Y_1 \cup Y_2$
 mit Y_1, Y_2 alg. Teilmengen $\Rightarrow Y = Y_1$ oder $Y = Y_2$

Z.B. $z = w^2$ ist irred, $zw = 0$ ist reduzibel.

Für $Y \subset K^n$ betrachte nun $I(Y) = \{P \in K[X_1, \dots, X_n] : \forall z \in Y, P(z) = 0\}$

Dies ist ein Ideal. Ist $Y \subset K^n$ alg. so heißt $K[X_1, \dots, X_n]/I(Y)$
 der Koordinatenring von Y .

Hilbertscher Nullstellensatz. Ist $\mathcal{O} \subset K[X_1, \dots, X_n]$, so gilt

$$I(Z(\mathcal{O})) = \text{rad } \mathcal{O} := \{P \in K[X_1, \dots, X_n] : \exists n \in \mathbb{N}, P^n \in \mathcal{O}\}$$

Korollar Die Korrespondenz

$$\{\text{alg. Teilmengen}\} \longleftrightarrow \{\mathcal{O} \subset K[X_1, \dots, X_n] : \mathcal{O} = \text{rad } \mathcal{O}\}$$

$$Y \longmapsto I(Y)$$

$$Z(\mathcal{O}) \longleftarrow \mathcal{O}$$

ist bijektiv. Y ist irred $\Leftrightarrow I(Y)$ prim $\Leftrightarrow K[X_1, \dots, X_n]/I(Y)$
 Integritätsring

2.5 Der Satz von Gauss

2.5.1 Satz R faktoriell $\Rightarrow R[X]$ faktoriell

Vorbereitungen:

2.5.2 Satz und Def. Sei R ein Integritätsring. Dann gilt:

(i) Durch $(a, b) \sim (a', b') : \Leftrightarrow ab' = a'b$ wird eine Äquival.
 auf $R \times (R \setminus \{0\})$ erklärt.

(ii) Sei $Q(R) = R \times (R \setminus \{0\}) / \sim$, $\frac{a}{b}$ = Klasse von (a, b) .

Definiere Verknüpfungen $+$, $\cdot$ auf $Q(R)$ durch $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$
 $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$. Diese sind wohldefiniert.

(iii) $(Q(R), +, \cdot)$ ist ein Körper, genannt Quotientenkörper von R .

(iv) $R \rightarrow Q(R), a \mapsto \frac{a}{1} \in Q(R)$ inj. Ringhomom., R wird also mit einem Subring von $Q(R)$ identifiziert.

2.5.3 Bsp. $Q(\mathbb{Z}) = \mathbb{Q}$, $Q(K[X]) = \left\{ \frac{P}{Q} : P, Q \in K[X], Q \neq 0 \right\} =: K(X)$
 heißt Körper der rationalen Fkt in einer Variabel mit Koeff. in K .

2.5.4 Def. Sei $f \in R[X]$, $c(f)$ = der ggT der Koeff von f , (bis auf Assoziiertheit eindeutig bestimmt). Wir können daher $f = c(f)f^*$ schreiben, mit $c(f^*) = 1$. Polynome mit $c(f) = 1$ nennt man primitiv.

2.5.5 Lemma (von Gauss) Für $f, g \in R[X]$ gilt $c(fg) = \varepsilon c(f)c(g)$ mit $\varepsilon \in R^*$. Sind f, g primitiv, so ist fg primitiv.

Beweis Schreibe $f = c(f)f^*$, $g = c(g)g^*$, $fg = c(f)c(g)f^*g^*$.
 Es reicht den zweiten Teil zu zeigen (ist f^*g^* primitiv, so $(fg)^* = f^*g^*$ und $c(f)c(g) = \varepsilon c(fg)$, $\varepsilon \in R^*$). Seien f, g primitiv.
 Ist fg nicht primitiv, so $\exists p \in R$ mit $p \mid c(fg)$.

Schreibe $f = \sum a_i X^i$, $g = \sum b_j X^j$, $fg = \sum \left(\sum_{i+j=k} a_i b_j \right) X^k$

Es seien a_r, b_s die ersten nicht durch p teilbaren Koeff. von f bzw. g . Dann gilt

$$\sum_{i+j=r+s} a_i b_j \equiv \sum_{\substack{i+j=r+s \\ i \geq r, j \geq s}} a_i b_j = a_r b_s \not\equiv 0 \pmod{p} \quad \downarrow$$