<u>Bem</u> zu Polynomringen in beliebig vielen Variablen.

Sei K ein Körper. Sei I eine Menge, nicht notwendig endlich. Sei $T = (T_i)_{i \in I}$ das Tupel unserer formalen Variablen. Wir wollen überprüfen, daß $K[T] = K[T_i : i \in I]$ ein Integritätsbereich ist.

Seien $f(T), \tilde{f}(T) \in K[T]^\times$.

Wir haben $f(T) \cdot \tilde{f}(T) \overset{!}{\neq} 0$ zu zeigen.

Dazu schreiben wir

$$f(T) = \sum_{t\in[1,\ell]} \underbrace{s_t}_{\in K} \, T_{i_{t,1}}^{e_{t,1}} \, T_{i_{t,2}}^{e_{t,2}} \cdot \ldots \cdot T_{i_{t,k_t}}^{e_{t,k_t}}$$

$$\tilde{f}(T) = \sum_{t\in[1,\tilde{\ell}]} \underbrace{\tilde{s}_t}_{\in K} \, T_{\tilde{i}_{t,1}}^{\tilde{e}_{t,1}} \, T_{\tilde{i}_{t,2}}^{\tilde{e}_{t,2}} \cdot \ldots \cdot T_{\tilde{i}_{t,\tilde{k}_t}}^{\tilde{e}_{t,\tilde{k}_t}}$$

Nun sind $f(T)$ und $\tilde{f}(T)$ enthalten im Teilring

$$S := K[T_{i_{1,1}}, \ldots, T_{i_{\ell,k_\ell}}, T_{\tilde{i}_{1,1}}, \ldots, T_{\tilde{i}_{\tilde{\ell},\tilde{k}_{\tilde{\ell}}}}]$$

$$\subseteq K[T],$$

der ein Polynomring in endlich vielen Variablen ist.

Wir wissen:

R Integritätsbereich $\Rightarrow$ $R[X]$ Integritätsbereich.

Dies iteriert angewandt liefert, daß der Polynomring in endlich vielen Variablen über einem Körper ein Integritätsbereich ist.

Insbesondere ist S ein Integritätsbereich. Da nun auch $f(T), \tilde{f}(T) \in S^\times$ liegen, folgt $f(T) \cdot \tilde{f}(T) \neq 0$, wie benötigt.

Bsp zur Vereinigung von Idealen

Im Beweis zu Lemma 241

haben wir gebraucht, daß für

einen komm. Ring R und eine Kette

$$K \subseteq \{ J : J \trianglelefteq R \}$$

auch die Vereinigung

$$\bigcup K = \bigcup_{J \in K} J$$

wieder ein Ideal ist.

Das ist ein Spezialfall!

Im allgemeinen ist die

Vereinigungsmenge zweier Ideale <u>nicht</u> wieder ein Ideal.

Z.B. ist in $\mathbb{Z}$ die

Vereinigungsmenge

$(2) \cup (3) =: V$

kein Ideal: Es ist

$2, 3 \in V$, aber

es ist

$\underbrace{1 \cdot 2 + 1 \cdot 3}_{= 5} \notin V.$

<u>Bsp</u> zu algebraischer Abgeschlossenheit.

Es ist $\mathbb{R}$ nicht algebraisch abgeschlossen. Denn es ist z.B. $X^2+1 \in \mathbb{R}[X]$ ein irreduzibles normiertes Polynom von Grad ≥ 2.

Aber immerhin gibt es in $\mathbb{R}[X]$ <u>kein</u> irreduzibles normiertes Polynom von Grad ≥ 3.

Annahme, doch.

Sei $f(X) \in \mathbb{R}[X]$ irreduzibel

und normiert und vom

Grad $n := \deg(f(X)) \geq 3$.

Zerlege in $\mathbb{C}[X]$:

$$f(X) = (X - z_1) \cdot \ldots \cdot (X - z_n)$$

Dies ist mit $z_1, \ldots, z_n \in \mathbb{C}$

möglich, da $\mathbb{C}$ algebraisch

abgeschlossen ist und folglich

alle irreduziblen normierten

Polynome in $\mathbb{C}[X]$ den

Grad 1 haben.

Schreibe $f(X) = \sum_{j \geq 0} \underbrace{a_j}_{\in \mathbb{R}} X^j$.

Für $z \in \mathbb{C}$ wird

$$\overline{f(z)} = \overline{\sum_{j \geq 0} a_j z^j}$$

komplexe Konjugation

$$= \sum_{j \geq 0} \overline{a_j} \cdot \overline{z}^j$$

$$= \sum_{j \geq 0} a_j \overline{z}^j$$

$$= f(\overline{z})$$

Insbesondere:

$$f(z) = 0 \iff \overline{f(z)} = 0$$

$$\iff f(\overline{z}) = 0.$$

Es gibt nach Annahme keine reelle Nullstelle von f.

Es ist also $z_1 \in \mathbb{C} \setminus \mathbb{R}$.

Sei $$g(X) := \frac{f(X)}{X - z_1}.$$

Es ist $f(\overline{z}_1) = 0$, s.o.

Es ist $\overline{z}_1 - z_1 \neq 0$.

Also ist $g(\overline{z}_1) = 0$.

Sei $$h(X) = \frac{g(X)}{X - \overline{z}_1}.$$

Zusammen ist

$$h(X) = \frac{f(X)}{(X - z_1)(X - \overline{z}_1)}$$

Es ist $(X - z_1)(X - \bar{z}_1)$

$$= X^2 - (z_1 + \bar{z}_1) X + z_1 \bar{z}_1$$

$$= X^2 - 2\mathrm{Re}(z_1) X + |z_1|^2$$

$$\in \mathbb{R}[X].$$

Also ist auch $h(X) \in \mathbb{R}[X]$,

da die Polynomdivision zu

$$h(x) = \frac{f(x)}{X^2 - 2\,\mathrm{Re}(z_1) + |z_1|^2}$$

in $\mathbb{R}[X]$ stattfindet.

Folglich ist

$$\underbrace{f(X)}_{\deg \geq 3} = \underbrace{h(X)}_{\deg \geq 1} \cdot \underbrace{\left(X^2 - 2\,\mathrm{Re}(z_1) + |z_1|^2\right)}_{\deg = 2}$$

$\deg \geq 3 \Rightarrow \deg \geq 1 \Leftarrow \deg = 2$

Wir haben einen Widerspruch.

Bsp zum Vergleich.

In $\mathbb{F}_2[X]$ gibt es irreduzible normierte Polynome von Grad ≥ 3 (im Gegensatz zu $\mathbb{R}[X]$).

z.B. gibt es dort:

$X^3 + X + 1$

$X^4 + X + 1$

$X^5 + X^2 + 1$

$X^6 + X + 1$

$X^7 + X + 1$

usf.

nicht aber $X^5 + X + 1$, da $X^5 + X + 1 = (X^2+X+1)(X^3+X^2+1)$