Wiederholung:

$AB = BA$

$(AB)C = A(BC)$

$A(B+C) = AB + AC$

Sei $\mu \in K$

$A(\mu)B(\mu) = B(\mu)A(\mu)$

$(A(\mu)B(\mu))C(\mu) = A(\mu)(B(\mu)C(\mu))$

$A(\mu)(B(\mu)+C(\mu)) = A(\mu)B(\mu) + A(\mu)C(\mu)$

$A = a_0 + a_1 X + \ldots + a_n X^n \quad \leftrightarrow \quad (a_0, a_1, \ldots, a_n) \in K^{n-1}$

Schreibweise: $A = a_n \cdot a_{n-1} \cdot a_{n-2} \cdot \ldots \cdot a_1 \cdot a_0$ (wie 1er, 10er, 100er, etc.)

Beispiele: Sei $K = \mathbb{Z}_2$

$A = X^3 + X + 1 = 1011$

$B = X^4 + X^3 + X^2 = 11100$

$$A + B = \begin{array}{r} 1011 \\ 11100 \\ \hline 10111 \end{array} = X^4 + X^2 + X + 1$$

Beispiel, dass bei $1+1=0$ nicht 1 gemerkt wird:

$X^3 + X^3 = (1+1)X^3 = 0$

$$A \cdot B = (1011)(11100)$$

$$\begin{array}{r} 1011 \\ 1011 \\ 1011 \\ 0000 \\ 0000 \\ \hline 1100010 0 \end{array} = X^7 + X^6 + X^2$$

Dividieren mit Rest:

$K = \mathbb{Z}_2, \; A = 110101 = X^5 + X^4 + X^2 + 1$

$B = 1011 = X^3 + X + 1$

$(1101\,01) \div (1011) = 111$

$$\begin{array}{r} 1011 \\ \hline 011001 \\ 10110 \\ \hline 01111 \\ 1011 \\ \hline 0100 \end{array} = X^2$$

$K = \mathbb{Z}_3$, A und B wie oben

$(1\,1\,0\,1\,0\,1) \div (1011) = 112$

$1\,0\,1\,1$

$01\,2\,0\,0\,1$

$1\,0\,1\,1$

$0\,2\,2\,2\,1$

$2\,0\,2\,2$

$0\,2\,0\,2 = 2X^2 + 2 = -X^2 - 1$

2.1. Satz

Sei $N \neq 0$ aus $K[X]$

$n = \operatorname{grad} N$.

Zu $A \in K[X]$ existieren eindeutig bestimmte Polynome $P, R \in K[X]$

und $A = PN + R$, $\operatorname{grad} R < n$

Beweis: Eindeutigkeit

$(A = P'N + R',\ \operatorname{grad} R' < n)$

$$\underbrace{0}_{\operatorname{grad} 0 = -1} = A - A = \underbrace{(P - P')}_{\geq n} N + \underbrace{(R - R')}_{< n}$$

$$\Rightarrow P - P' = 0$$

$$\Rightarrow P = P$$

$$\Rightarrow R = R'$$

Beispielprogramm für Algorithmus:

START $R := A$

$P := 0$

$\lambda :=$ Leitkoeffizient von N

WHILE $\operatorname{grad} R \geq n$ DO

$m := \operatorname{grad} R$

$\mu :=$ Leitkoeffizient von R

$$R := R - \frac{\mu}{\lambda} X^{m-n} N$$

$$P := P + \frac{\mu}{\lambda} X^{m-n}$$

END

$R = \rho_n(A)$ Rest modulo N

$\langle N \rangle = \{ PN \mid P \in K[X] \}$

$A - \rho_N(A) \in \langle N \rangle$

$\rho_N : K[X] \to K_n[X],\ A \mapsto \rho_N(A)$ Restabbildung

Sei $\rho := \rho_N$

2.2. a) $\rho(A) = A \Leftrightarrow A \in K_n[X]$

b) $\rho(A) = 0 \Leftrightarrow A \in \langle N \rangle$

c) $\rho(A) = \rho(B) \Leftrightarrow A - B \in \langle N \rangle$

d) ρ ist eine lineare Abbildung

$$\rho(\lambda A + \mu B) = \lambda\rho(A) + \mu(\rho(B))$$

e) $\rho(A \cdot B) = \rho(\rho(A) \cdot \rho(B))$

Beweis:

a) - c) offensichtlich

zu d) $A_0 := \rho(A),\ B_0 = \rho(B)$

$$A = PN + A_0,\ B = QN + B_0$$

$$\lambda A + \mu B = (\lambda P + \mu Q)N + \underbrace{(\lambda A_0 + \mu B_0)}_{\in K_n[X]}$$

$$\Rightarrow \rho(\lambda A + \mu B) = \lambda A_0 + \mu B_0$$

zu e) $A \cdot B = \underbrace{PQNN + PNB_0 + A_0QN}_{\in \langle N \rangle} + A_0B_0$

$$A \cdot B - A_0 \cdot B_0 \in \langle N \rangle$$

Behauptung folgt aus c)

$$A \equiv B \pmod N \overset{\text{def.}}{\Leftrightarrow} \rho_N(A) = \rho_N(B) \overset{\text{c)}}{\Leftrightarrow} A - B \in \langle N \rangle$$

2.3. Satz

Sei $A \in K[X]$ und $\lambda \in K$ eine Nullstelle von A, d.h. $A(\lambda) = 0$.

Dann existiert $P \in K[X]$ mit $A = (X - \lambda)P$

Beweis:

1. Fall: $\operatorname{grad} A \le 0 \Rightarrow A = 0$

2. Fall: $\operatorname{grad} A > 0$

Teile A durch $X - \lambda$

$$A = P(X - \lambda) + R,\ \operatorname{grad} R \le 0$$

$$0 = A(\lambda) = P(\lambda)(\lambda - \lambda) + R(\lambda)$$

$$\Rightarrow R = 0$$

Sei $A(\lambda) = 0$, d.h. $A = (X - \lambda)P$

Sei $\mu \neq \lambda$ eine weitere Nullstelle

$$0 = A(\mu) = \underbrace{(\mu - \lambda)}_{\neq 0}\underbrace{P(\mu)}_{=0}$$

$$\Rightarrow P = (X - \mu)Q,\ Q \in K[X]$$

$A = (X-\lambda)(X-\mu)Q$ (usw. mit immer neuen Nullstellen)

2.4. Korollar

Sei $\lambda_1,...,\lambda_m$ verschiedene Nullstellen von A

Dann existiert $P \in K[X]$ mit $A = (X-\lambda_1)(X-\lambda_2)...(X-\lambda_m)P$

Insbesondere mit $m \leq \text{grad } A$

Ein Polynom vom grad n hat höchstens n Nullstellen.

$\mathbb{Z}_n = \{0,1,...,n-1\}$

Sei $n \geq 1$ und N ein Polynom vom Grad n

Wir machen $K_n[X]$ zu einem Ring via ρ_N

$A, B \in K_n[X]$

$A +_N B = A + B$

$A \cdot_N B \overset{\text{def.}}{=} \rho_N(A \cdot B)$

2.5. Bezüglich dieser Addition und Multiplikation ist $K_n[X]$ ein kommutativer Ring.

Wir bezeichnen ihn mit K_N (z.B. $\mathbb{Z}_N$)

Beachte: K_N ist insbesondere K-Vektorraum der Dimension n ($= K_n[X]$)

K-Algebra

Beispiel:

$K = \mathbb{R}$, $N = X^2 + 1 \in \mathbb{R}[X]$

$X^2 = X \cdot_N X = 1 \cdot N + (-1)$

$X \cdot_N X = -1$

$a_1 + b_1 X = a_2 + b_2 X \in K_2[X]$

$$(a_1 + b_1 X) \cdot_N (a_2 + b_2 X) = \rho_N((a_1 + b_1 X)(a_2 + b_2 X))$$
$$= \rho_N(a_1 a_2 + (a_1 b_2 + b_1 a_2) X + b_1 b_2 X^2)$$
$$\overset{\text{z.z.d}}{=} \rho(a_1 a_2) + \rho((a_1 b_2 + b_1 a_2) X + b_1 b_2 \rho(X^2))$$
$$= a_1 a_2 + (a_1 b_2) X + (b_1 a_2) X + b_1 b_2$$
$$= (a_1 a_2 - b_2 b_1) + (a_1 b_2 + b_1 a_2) X$$

Sei z.B. $i := X$

$(a_1 + i b_1)(a_2 + i b_2) = (a_1 a_2 - b_2 b_1) + (a_1 b_2 + b_1 a_2) i$