$N \in K[X] \geq 1$

$K_n = K_n[X]$

$A \cdot_n B = \rho_N(AB)$

Beispiel: 1. $K = \mathbb{R},\ N = X^2 + 1 \Rightarrow K_N = \mathbb{C}$

$K = \mathbb{Z}_2 = \{0,1\}$

$K_2[X] = \{0,1,X,X+1\}$

2. $N = X^2 + 1$

$(X+1) \cdot_N (X+1) = \rho_N\left((X+1)^2\right) = 0$

$(X+1)^2 = (X+1)(X+1)$

$= X^2 + 1 + X + X$

$= X^2 + 1 + X(1+1)$

$= X^2 + 1$

3. $N = X^2 + X = X(X+1)$

$X \cdot_N (X+1) = 0$

4. $N = X^2 + X + 1$

$X^2 = 1N + X + 1$

$X \cdot_N X = X + 1$

	1	X	X+1
1	1	X	X+1
X	X	X+1	1
X+1	X+1	1	X

$X(X+1) = X^2 + X = N + 1$

$(X+1)(X+1) = X^2 + 1 = N + X$

5. $n = 3,\ K = \mathbb{Z}_2,\ N = X^3 + X + 1 \in K[X]$

$K_N = \{000,100,010,001,110,101,011,111\}$

$\rho_N(X^3) = 110$

$\rho_N(X^4) = \rho_N(X^3 \cdot X) = \rho\left(\rho(X^3)\underbrace{\rho(X)}_{X}\right)$

$= \rho((1+X)X) = \rho(X^2 + X) = X^2 + X$

$K = \mathbb{Z}_2 = \{0,1\}$

$N = X^3 + X + 1 \in K[x]$

$A = a_0 + a_1 X + a_2 X^2 \in K_N$

$= a_0 a_1 a_2$

Multiplikationstafel von K_N

N	100	110	010	111	011	101	001
100	100	110	010	111	011	101	001
110	110	101	011	010	100	001	111
010	010	011	001	101	111	100	110
111	111	010	101	110	001	011	100
011	011	100	111	001	010	110	101
101	101	001	100	011	110	111	010
001	001	111	110	100	101	010	011

Bemerkungen:

- $K_1[X] = X \leq K_N[X]$ K ist immer Unterraum von K_N
- Im Fall $n = 1$ ist $K_N = K$

2.6. Satz

Genau dann ist der Ring K_N ein Körper, wenn K_N nullteilerfrei ist. (Vgl. 1.5.)

Beweis: $A \cdot B$ statt $A \cdot_N B$

Sei $A \neq 0$ in K_N fixiert, gesucht ist ein $B \in K_N$ mit $A \cdot B = 1$

$\varphi : K_N \to K_N$ mit $B \mapsto AB$

1. φ ist injektiv: $\varphi(B) = \varphi(C) \Rightarrow AB = AC$

   $\overset{\text{Kürzregel}}{\underset{\text{da nullteilerfrei}}{\Rightarrow}} B = C$

2. φ ist linear:

   $\varphi(\lambda B + \mu C) = A(\lambda B + \mu C) = \lambda AB + \mu AC$

   $= \lambda\varphi(B) + \mu\varphi(C)$

3. φ ist bijektiv:

   $n = \dim K_N[X] = \dim \operatorname{im}\varphi + \dim \ker\varphi$

   $\Rightarrow \operatorname{im}\varphi = K_N \to$ surjektiv

Anhang 1: Das Ableitungskalkül

$A = a_0 + a_1 X + .. + a_n X^n$

$A' \overset{\text{def.}}{=} a_1 + \underbrace{(a_2 + a_2)}_{2a_2} X + ... + \underbrace{(a_n + ... + a_n)}_{n \cdot a_n} X^{n-1}$

2.7. Die Abbildung $A \to A'$ vom $K_N[X]$ ist linear

und ergibt $(AB)' = A'B + AB'$ **Produktregel**

$$K[X,Y] = \left\{ \sum_{(i,j)\in\mathbb{N}_0\times\mathbb{N}_0} a_{ij} X^i Y^j \,\middle|\, a_{ij} \in K \right\}$$

In einem Polynom $A(X) = \sum a_i X^i$ können wir $X + Y \in K[X,Y]$ einsetzen und

$$\begin{aligned} A(X+Y) &= a_0 + a_1(X+Y) + a_2(X+Y)^2 + \ldots \\ &= a_0 + a_1 X + a_1 Y + a_2 X^2 + 2a_2 XY + a_2 Y^2 + \ldots \\ &= A(X) + (a_1 + 2a_2 X + \ldots)Y + (a_2 + \ldots)Y^2 + \ldots \\ &= A(X) + A_1(X)Y + Y^2(\ldots) \end{aligned}$$

A' ist Ableitung von A

z.B. $A = X^n$

$$A(X+Y) = (X+Y)^n = X^n + nX^{n-1}Y + Y^2(\ldots)$$

$$(XA)(X+y) = (\lambda A)(X) + (\lambda A_1)(X)Y + \lambda Y^2(\ldots)$$

$$(\lambda A)' = \lambda A_1 = \lambda A'$$

$$(A+B)(X+Y) = (A+B)(X) + \left(A_1(X) + B_1(X)\right)Y + Y^2(\ldots)$$

$$A + B' = A' + B$$

$$\begin{aligned} (AB)(X+Y) &= A(X+Y)B(X+Y) \\ &= \left(A(X) + YA'(X) + Y^2(\ldots)\right)\left(B(X) + B'(X)Y + Y^2(\ldots)\right) \\ &= A(X)B(X) + Y\left(A'(X)B(X) + A(X)B'(X) + Y^2(\ldots)\right) \end{aligned}$$

2.8. Sei $A \neq 0$ aus $K[X]$ und λ Nullstelle von A

Äquivalent sind:

i) λ ist einfache Nullstelle von A

($(x-\lambda)$ aber nicht $(X-\lambda)^2$ ist Teiler von A)

ii) $A'(\lambda) \neq 0$

Wir wissen: $A(X) = (X-\lambda)P$

$$(X-\lambda)^2 \text{ teilt } A \overset{\text{Kürzregel}}{\Leftrightarrow} X - \lambda \text{ teilt } P \Leftrightarrow P(\lambda) = 0$$

$$A' = \underbrace{(X-\lambda)'}_{1} P + (X-\lambda)P'$$

$$\begin{aligned} A'(\lambda) &= P(\lambda) \\ &= 0 \Leftrightarrow P(\lambda) = 0 \end{aligned}$$

„Regel von de l'Hospital"

Gegeben: $A,B,C \in K[X]$: $A \cdot B = C \quad (\lambda \in K)$

$$A(\lambda)B(\lambda) = C(\lambda),\ A(\lambda) = \frac{C(\lambda)}{B(\lambda)} \text{ falls } B(\lambda) \neq C$$

Voraussetzung: Sei $B(\lambda) = 0$, aber λ einfache Nullstelle von B

Behauptung: $A(\lambda) = \frac{C'(\lambda)}{B'(\lambda)}$

Beweis: $C' = (AB)' = A'B + AB'$

$$C'(\lambda) = \underbrace{A'(\lambda)B(\lambda)}_{0} + A(\lambda)B'(\lambda)$$

Sei R (kommutativer) Ring

$$R[X] = \left\{ \sum_{i=0} a_i X^i \,\middle|\, a_i \in R \right\} \text{ (Polynomring über } R)$$

$$R[X_1,...,X_n] = \left\{ \sum_{(i_1,...,i_n)\in \mathbb{N}_0{}^n}^{\text{endlich}} a_{i_1...i_n} X_1^{i_1} X_2^{i_2} ....X_n^{i_n} \,\middle|\, a_{i_1...i_n} \in R \right\}$$

R sei **Unterring** eines Rings S (z.B. $R = \mathbb{Z},\ S = \mathbb{Q}$)

$s_1,...,s_n \in S$

$$R[s_1,...,s_n] \overset{\text{def.}}{=} \left\{ \sum_{i_1...i_n}^{\text{endlich}} a_{i_1...i_n} \cdot s_1^{i_1} s_2^{i_2} ...s_n^{i_n} \right\} \leq S$$

ist der kleinste Unterring von S, welcher R und die Elemente $s_1,...,s_n$ enthält.