3.5. $\underbrace{\mathrm{ggT}(A,B)}_{G} = A \Rightarrow \mathrm{kgV}(A,B) = AB \quad (\text{im Fall } G \neq 1)$

3.6. $\mathrm{kgV}(A,B) = A \cdot \frac{B}{G} = \frac{A}{G} \cdot B$

Beispiel: $A = 12,\ B = 18,\ G = 6$

$\mathrm{kgV}(A,B) = 12 \cdot 3 = 2 \cdot 18$

$N \in K[X],\ \mathrm{grad}\, N = n \geq 1$

N **irreduzibel (unzerlegbar)**, wenn N keinen nichttrivialen Teiler besitzt.

Beispiel: Polynome vom Grad 1 sind irreduzibel

- Sei N irreduzibel und $A \neq 0$
  Dann $A \in \langle N \rangle$ oder $\mathrm{ggT}(A,N) = 1$
- Bezeichnung: $\mathcal{P}(A)$ Menge der (normierten) irreduziblen Polynome, welche A teilen.

3.7. Satz

Prim (Eigenschaft): $\mathcal{P}(AB) = \mathcal{P}(A) \cup \mathcal{P}(B)$

Beweis: $N \in \mathcal{P}(AB)$

$K = \mathrm{kgV}(A,B) \quad AB \in \langle K \rangle$

Sei N kein Teiler von $A \Rightarrow \mathrm{ggT}(A,N) = 1$

$\overset{3.5.}{\Rightarrow} K = AN \qquad AN$ Teiler AB

Bemerkung im Allgemeinen:

Sei R kommutativer Ring $p \in R$ heißt **Primelement**,

wenn $p/ab \Rightarrow p/a$ oder p/b

p Primelement $\Rightarrow$ p ist unzerlegbar

Konsequenzen I-III

I) $K_N \quad A \cdot_N B = \rho_N(AB) = 0$

K_N ist nullteilerfrei $\Leftrightarrow$ N irreduzibel

3.8. Satz

Der Ring K_N ist genau dann ein Körper, wenn N irreduzibel ist.

II) Definiere das direkte Produkt von Ringen S, T

$R = S \times T = \{(s,t) \mid s \in S,\ t \in T\}$

Addition und Multiplikation komponentenweise

ACHTUNG: Entsetzlich viele Nullteiler

Sei $N = N_1 N_2$ in $K[X]$, $\operatorname{grad} N \geq 1$

Bilde $R = K_{N_1} \times K_{N_2}$

$\varphi : K_N \to R$

$\varphi(P) = \left(\rho_{N_1}(P), \rho_{N_2}(P)\right)$

3.9. Ringhomomorphismus

$$\begin{aligned}\varphi(P+Q) &= \left(\rho_{N_1}(P+Q), \rho_{N_2}(P+Q)\right)\\ &= \left(\rho_{N_1}(P) +_{N_1} \rho_{N_1}(Q), \rho_{N_2}(P) +_{N_2} \rho_{N_2}(Q)\right)\\ &= \varphi(P) + \varphi(Q)\end{aligned}$$

$$\begin{aligned}\varphi(P \cdot_N Q) &= \varphi\left(\rho_N(PQ)\right) = \left(\rho_{N_1}\left(\rho_N(PQ)\right), \rho_{N_2}\left(\rho_N(PQ)\right)\right)\\ &= \left(\rho_{N_1}(P) \cdot_{N_1} \rho_{N_1}(Q), \rho_{N_2}(P) \cdot_{N_2} \rho_{N_1}(Q)\right)\end{aligned}$$

3.10. Chinesischer Restsatz

Sei $N = N_1 N_2$ mit teilerfremden Polynomen N_1, N_2.

Dann ist φ Bijektion also ein **Ring-Isomorphismus** $K_{N_1} \times K_{N_2} \cong K_N$

Beweis: Sei $\varphi(P) = (0,0)$

$\rho_{N_1}(P) = \rho_{N_2}(P) = 0$

N_1 / P und $N_2 / P \Rightarrow \operatorname{kgV}(N_1, N_2)$ Teiler v.P.

$$\underset{\|}{N_1} - N_2 = N \quad \Rightarrow P = 0$$

Andere Formulierung

Sei $L_1 \in K_{N_1}$, $L_2 \in K_{N_2}$, $\operatorname{grad} L < n$

$\exists$ genau eine Lösung $L \in K_N$ mit $L \equiv L_1 \bmod N_1$

$L \equiv L_2 \bmod N_2$

Rezept: $\operatorname{ggT}(N_1, N_2) = 1$: $\exists P_1, P_2$ mit $1 = P_1 N_1 + P_2 N_2$

$$P_1 N_1 \equiv \begin{cases} 1 \bmod N_2 \\ 0 \bmod N_1 \end{cases}$$

$$P_2 N_2 \equiv \begin{cases} 1 \bmod N_1 \\ 0 \bmod N_2 \end{cases}$$

$\tilde{L} := L_1 P_2 N_2 + L_2 P_1 N_1$ ist Lösung

$\tilde{L} = TN + L$, $\operatorname{grad} L < n$

$L \equiv \tilde{L} \bmod N_1, N_2$

Beispiel: $n_1 = 5,\ n_2 = 9,\ n = 45$

$l_1 = 3,\ l_2 = 5,\ l = ?$

$l \equiv l_1 \bmod 5$

$l \equiv l_2 \bmod 9$

$1 = 2 \cdot 5 + (-1) \cdot 9$

$\tilde{l} = 3 \cdot (-1) \cdot 9 + 5 \cdot 2 \cdot 9 = 23$

$N = N_1, N_2, ..., N_m,\ \text{ggT}(N_i, N_j) = 1,\ \text{für } i \neq j$

Gegeben: $L_1, ..., L_m \in K[X]$

$L \equiv L_1 \pmod{N_1}$

$L \equiv L_2 \pmod{N_2}$

$\vdots$

$L \equiv L_m \pmod{N_m}$

$\Rightarrow \exists$ genau eine Lösung L mit grad $L < n$

III) Satz von der eindeutigen Primfaktorzerlegung

$N \in K[X]$, grad $N \geq 1$, normiert $(n \in \mathbb{N}, n > 1)$

$\mathcal{P}(N)$ Menge der normierten irreduziblen Teiler von N

1) $N = \prod_{P \in \mathcal{P}(N)} P^{e_p}, \quad e_p \in \mathbb{N} \qquad 12 = 2^2 \cdot 3$

Beweis (Induktion):

N irreduzibel $\surd$

N nicht irreduzibel:

$N = N_1 N_2,\ N_i$ normiert

$1 \leq \text{grad } N_i < \text{grad } N$

$N = \prod_{p \in \mathcal{P}(N_1)} p^* \prod_{p \in \mathcal{P}(N_2)} p^*$

2) Sei D die Menge aller normierten Teiler von N und

$\tilde{D} = \left\{ (f_p)\, p \in \mathcal{P}(N) \middle| 0 \leq f_p \leq e_p \right\}$

Behauptung: Die Abbildung $\beta : \tilde{D} \to D$ mit

$(f_p)_{p \in \mathcal{P}(N)} \mapsto \prod_{p \in \mathcal{P}(N)} P^{f_p}$ ist eine Bijektion

Beweis:

β ist surjektiv:

Sei A normierter Teiler von N, also $A \in D$

$\mathcal{P}(A) \subseteq \mathcal{P}(N)$

$$A = \prod_{p \in \mathcal{P}(A)} P^{f_p}$$

z.Z.: $f_p \leq e_p$

Annahme: $f_p > e_p$ für ein $p_1 \in \mathcal{P}(A)$

$$p_1^{f_{p_1}} \prod_{p \in \mathcal{P}(A) \setminus \{p_1\}} p^{f_p} \text{ teilt } p_1^{e_{p_1}} \prod_{p \in \mathcal{P}(A) \setminus \{p_1\}} p^{e_p}$$

$$p_1^{f_{p_1} - e_{p_1}} \prod_{p \in \mathcal{P}(A) \setminus \{p_1\}} p^{f_p} \text{ teilt } p_1^{e_{p_1}} \prod_{p \in \mathcal{P}(A) \setminus \{p_1\}} p^{e_p}$$

$\text{prim} \Rightarrow p_1 \in \mathcal{P}(N) \setminus \{p_1\}$ ↯

β ist injektiv:

$$\prod_{p \in \mathcal{P}(A)} P^{e_p} = \prod_{p \in \mathcal{P}(A)} P^{f_p} \quad \Rightarrow \; e_p = f_p \quad \forall p$$

$ep_1 < fp_1$ für ein p_1

$$P_1^{e_{p_1}} \prod_{p \neq p_1} P = P_1^{f_{p_1}} \prod_{p \neq p_2}$$

... p_1 teilt $\prod P$ ↯ $p \neq p_1$

zu Primeigenschaft