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

$r +_n s = \rho_n(r+s) \quad r,s \in \mathbb{Z}$ modulo

$r \cdot_n s = \rho_n(r \cdot s)$

$\mathbb{Z}_n$ ist kommutativer Ring

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

$\mathbb{Z}_5$:

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot_5$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

1.5. Genau dann ist der Ring $\mathbb{Z}_n$ nullteilerfrei, wenn n Primzahl ist.

Beweis: $u = r \cdot s,\ r,s \in \mathbb{Z}_n$

$r \cdot_n s = \rho_n(n) = 0$ $\exists$ ein Nullteiler

Sei n Primzahl

Annahme: $r \cdot_n s = 0$ für $0 \neq r,s \in \mathbb{Z}_n$

$\rho_n(rs) = 0$

$p = n$ teilt $rs \overset{!!!}{\Rightarrow} p$ teilt r oder p teilt s

$n = p \mid r \cdot s$

$n = 12$ Teiler von $12 = 2 \cdot 6$

$n = 5$ Teiler von $25 \cdot 13$

Sei R Ring

$R^* := \{r \in R \mid r \neq 0\}$

- R ist nullteilerfrei $\Leftrightarrow\ r,s \in \mathbb{R}^* \ \Rightarrow\ r,s \in R^*$
- In einem nullteilerfreien Ring kann gekürzt werden

$$r \neq 0,\ r \cdot s = r \cdot t \ \Rightarrow s = t$$

$$0 = rs - rt = \underbrace{r}_{\neq 0}\underbrace{(s-t)}_{=0}$$

1.6. Satz

Der Ring $\mathbb{Z}_n$ ist genau dann ein Körper (d.h. $\mathbb{Z}_n^*$ ist Gruppe bzgl. der Multiplikation) wenn n eine Primzahl ist.

Beweis: Sei n eine Primzahl, also $\mathbb{Z}_n$ ist nullteilerfrei

$r \neq 0 \quad M := \{r \cdot_n s \,|\, s \in \mathbb{Z}_n\}$

Behauptung: $|M| = n \ \Rightarrow\ M = \mathbb{Z}_n \overset{1 \in \mathbb{Z}_n}{\Rightarrow}$ es existiert s mit $r \cdot_n s = 1$

$$\left.\begin{array}{l} r \cdot_n s_1 = r \cdot_n s_2 \\ \Rightarrow\ s_1 = s_2 \end{array}\right\} n \text{ verschiedene } s \ \Rightarrow\ |M| = n$$

2. Der Polynomring

Sei K ein Körper

$A = A(X) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n$ Rechenausdruck, in der man für die Variable x Zahlen $\mu \in K$ einsetzen kann (u.a.)

$A(\mu) := a_0 + a_1\mu + a_2\mu^2 + \ldots + a_n\mu^n \in K$

Im Falle $a_n \neq 0$ ist $\operatorname{grad} A = n$

a_n ist **Leitkoeffizient** von A

Sind alle $a_i = 0$, so ist $A = 0$ das **Nullpolynom**

$\operatorname{grad} 0 := -1$

$\operatorname{grad} A = 0 : A = a_0,\ a_0 \neq 0$ **konstantes Polynom**

$K[x]$ ist die **Menge aller Polynome** über K

$B = b_0 + b_1 x + \ldots + b_m x^m \in K[x] \quad \lambda \in K$

$\lambda A(\mu) = \lambda a_0 + (\lambda a_1)\mu + (\lambda a_2)\mu^2 + \ldots$

$A(\mu) + B(\mu) = (a_0 + b_0) + (a_1 + b_1)\mu + (a_2 + b_2)\mu^2 + \ldots$

$A(\mu)B(\mu) = a_0 b_0 + (a_0 b_1 + b_0 a_1)\mu + (a_0 b_2 + a_1 b_1 + a_2 b_0)\mu^2 + \ldots$

Deswegen definiert man

$\lambda A := (\lambda a_0) + (\lambda a_1)x + \ldots + (\lambda a_n)x^n$

$A + B := \sum (a_i + b_i) x^i$

$AB := \sum c_i x^i \quad c_i = a_0 b_i + a_1 b_{i-1} + \ldots + a_{i-1} b_1 + a_i b_0$

Insbesondere $x^i x^j = x^{i+j}, \quad i, j \in \mathbb{N}^0$

$x^0 := 1$

$\Rightarrow$ **1. Einsetzungsregel:**

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

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

2. Gradformel:

$\operatorname{grad} \lambda A = \operatorname{grad} A,$ wenn $\lambda \neq 0$

$\operatorname{grad} AB = \operatorname{grad} A + \operatorname{grad} B,$ wenn $A, B \neq 0$

$\operatorname{grad}(A+B) \leq \max\{\operatorname{grad} A, \operatorname{grad} B\}$ mit Gleichheit, wenn $\operatorname{grad} A \neq \operatorname{grad} B$

3. Bzgl. der Addition & Skalarprodukt ist $K[x]$ ein **K-Vektorraum** (mit Basis $1 = x^0, x, x^2, \ldots$)

$$K[x] = \left\{ (a_i)_{i \in \mathbb{N}_0} \,\middle|\, \exists n \in \mathbb{N}_0 \text{ mit } a_i = 0 \ \forall i \geq n \right\}$$

4. Bzgl. der Addition & Multiplikation ist $K[x]$ **kommutativer, nullteilerfreier Ring**

Nullteilerfrei:	$A, B \neq 0$
	$\operatorname{grad} AB = \operatorname{grad} A + \operatorname{grad} B \geq 0$
Einselement:	$1 = x^0 \geq 0$
Distributivgesetz:	$A(B+C) = AB + AC$
Assoziativgesetz:	
zusätzlich:	$\lambda(AB) = (\lambda A)B = A(\lambda B)$
	***K*-Algebra**

5. Für $A \in K[x]$ sei $\langle A \rangle := \{ PA \,|\, P \in K[x] \}$ **Menge aller Vielfachen von *A***

a) $\langle A \rangle$ ist Unterraum des VRs $K[x]$ $\qquad \lambda(P_1 A) + \mu(P_2 A) = (\lambda P_1 + \mu P_2) A$

b) $B \in \langle A \rangle,\ Q \in K[x] \Rightarrow QB \in \langle A \rangle$ $\qquad B = PA,\ QB = Q(PA) = (QP)A$

siehe 1.1. d.h. $\langle A \rangle$ ist **Ideal** im Ring $K[x]$

6. $n \in \mathbb{N}$: $\quad K_n[x] = \{ A \in K[x] \,|\, \operatorname{grad} A < n \}$

$A = a_0 + a_1 x + \ldots + a_{n-1} x^{n-1}$

$K_n[x]$ ist Unterraum des Vektorraums $K[x]$

$(1, x, x^2, \ldots, x^{n-1}$ ist eine Basis von $K_n[x])$

$\dim K_n[x] = n$

Die Abbildung $K^n \to K_n[x]$ mit $(a_0, \ldots, a_{n-1}) \mapsto \sum_{i=0}^{n-1} a_i x^i$ ist Isomorphismus des Vektorraums K^n auf $K_n[x]$