

28.11.05

Ring $(\mathbb{R}, +, \cdot)$ Restklassen modulo $m \in \mathbb{N} \setminus \{1\}$ $a, b \in \mathbb{Z}$

$$m \mid b - a$$

$$a \equiv b \pmod{m}$$

$$\Leftrightarrow a \equiv b \pmod{m}$$

Bezeichnung: $a \in \mathbb{Z}$ $\bar{a}$ Äquivalenzklasse (Restklasse) die a enthält $\mathbb{Z}_m = \mathbb{Z} / m \mathbb{Z}$ Menge der Restklassen

Addition: $\bar{a} + \bar{b} = \overline{a+b}$

wohldefiniert: $a = \tilde{a}(m), b = \tilde{b}(m) \Rightarrow m \mid \tilde{a} - a, m \mid \tilde{b} - b$

$$\Rightarrow m \mid (\tilde{a} - a) + (\tilde{b} - b) = (\tilde{a} + \tilde{b}) - (a + b)$$

$$\Rightarrow a + b = \tilde{a} + \tilde{b} \pmod{m}$$

 $(\mathbb{Z}_m, +)$ additive Gruppe

assoziativ:
$$(\bar{a} + \bar{b}) + \bar{c} = \overline{a+b+c} = \overline{(a+b)+c} = \overline{a+(b+c)} = \overline{a+b+c} = \bar{a} + \overline{b+c} = \bar{a} + (\bar{b} + \bar{c})$$

kommutativ:
$$\bar{a} + \bar{b} = \overline{a+b} = \overline{b+a} = \bar{b} + \bar{a}$$

neutral
$$\bar{a} + \bar{0} = \overline{a+0} = \overline{0+a} = \bar{0} + \bar{a}$$

$$\bar{0} = m \mathbb{Z} = \{z : m \mid z\}$$

invers:
$$\bar{a} + \overline{m-a} = \overline{a+(m-a)} = \bar{m} = \bar{0}$$

Multiplikation:
$$\bar{a} \cdot \bar{b} = \overline{a \cdot b}$$

wohldefiniert:
$$\begin{aligned} a &\equiv \tilde{a}(m), b \equiv \tilde{b}(m) \Rightarrow m \mid \tilde{a} - a, m \mid \tilde{b} - b \\ \tilde{a} \cdot \tilde{b} - a \cdot b &= \tilde{a} \cdot \tilde{b} - a \cdot \tilde{b} + a \cdot \tilde{b} - a \cdot b = \\ &= (\tilde{a} - a) \tilde{b} + a(\tilde{b} - b), m \mid (\tilde{a} - a) \tilde{b}, m \mid a(\tilde{b} - b) \\ &\Rightarrow m \mid \tilde{a} \cdot \tilde{b} - a \cdot b \end{aligned}$$

assoziativ:
$$(\bar{a} \cdot \bar{b}) \cdot \bar{c} = \overline{ab \cdot c} = \overline{(a \cdot b) \cdot c} = \overline{a \cdot (bc)} = \bar{a} \cdot \overline{bc} = \bar{a} \cdot (\bar{b} \cdot \bar{c})$$

kommutativ:
$$\bar{a} \cdot \bar{b} = \overline{ab} = \overline{ba} = \bar{b} \cdot \bar{a}$$

dis)ributiv: $(\bar{a} + \bar{b}) \cdot \bar{c} = \overline{a+b} \cdot \bar{c} = \overline{(a+b) \cdot c} = \overline{ac+bc} = \overline{ac} + \overline{bc} = \bar{a} \cdot \bar{c} + \bar{b} \cdot \bar{c}$

Damit $(\mathbb{Z}_m, +, \cdot)$ ein kommutativer Ring mit 1: $\bar{a} \cdot \bar{1} = \overline{a \cdot 1} = \bar{a} = \overline{1 \cdot a} = \bar{1} \cdot \bar{a}$

$(\mathbb{Z}_m, +, \cdot)$ nullteilerfrei $\Leftrightarrow m$ Primzahl

" $\Rightarrow$ " Annahme $m = pq$ mit $p, q \in \mathbb{N} \setminus \{1\} \Rightarrow 1 < p, q < m \Rightarrow \bar{p}, \bar{q} \neq \bar{0}$
 $\bar{p} \cdot \bar{q} = \overline{pq} = \bar{m} = \bar{0}$

" $\Leftarrow$ " $\bar{p} \cdot \bar{q} = \bar{0} \Rightarrow m \mid p \cdot q \xrightarrow[\text{Primzahl}]{m} m \mid p \vee m \mid q \Rightarrow \bar{p} = \bar{0} \vee \bar{q} = \bar{0}$

□

Bemerkung $\mathbb{Z}_m = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{m-1}\} = \{\bar{1}, \bar{2}, \dots, \bar{m}\}$

4. $(R, +, \cdot)$ Ring, Matrizenringe $M_{n,n}^R$ für alle $n \in \mathbb{N}$ mit 1
 falls R Ring mit 1, nicht kommutativ

(additive)

5. A abelsche Gruppe. $\text{End } A$ Menge der Endomorphismen von A

$f: A \rightarrow A$ Endomorphismus $\Leftrightarrow f(a+\tilde{a}) = f(a) + f(\tilde{a})$ für alle $a, \tilde{a} \in A$
 $f(0) = 0, f(-a) = -f(a)$

Addition: $(f+g)(a) = f(a) + g(a)$

Endomorphismus:

$(f+g)(a+\tilde{a}) = f(a+\tilde{a}) + g(a+\tilde{a}) = f(a) + f(\tilde{a}) + g(a) + g(\tilde{a}) = f(a) + g(a) + f(\tilde{a}) + g(\tilde{a}) = (f+g)(a) + (f+g)(\tilde{a})$

$(\text{End}, +)$ abelsche Gruppe

assoziativ: $((f+g)+h)(a) = (f+g)(a) + h(a) = f(a) + g(a) + h(a) = f(a) + (g+h)(a) = (f+(g+h))(a)$

kommutativ: $(f+g)(a) = f(a) + g(a) = g(a) + f(a) = (g+f)(a)$

neutrales Element: $0: A \rightarrow A, a \mapsto 0 \quad (f+0)a = f(a) + 0 = f(a)$

invers: $(-f)(a) = -f(a)$

$$(-f)(a+\tilde{a}) = -f(a+\tilde{a}) = -(f(a) + f(\tilde{a})) = -f(a) + (-f(\tilde{a}))$$

$$(f + (-f))(a) = f(a) + (-f)(a) = f(a) + (-f(a)) = 0$$

Multiplikation: $(f \circ g)(a) = f(g(a))$

$$\begin{aligned} (f \circ g)(a+\tilde{a}) &= f(g(a+\tilde{a})) = f(g(a) + g(\tilde{a})) = f(g(a)) + f(g(\tilde{a})) \\ &= (f \circ g)(a) + (f \circ g)(\tilde{a}) \end{aligned}$$

$f \circ g = f \circ g$ Verkettung von Abbildungen ist assoziativ.

distributiv:

$$\begin{aligned} ((f+g) \cdot h)(a) &= (f+g)(h(a)) = f(h(a)) + g(h(a)) = \\ &= (f \cdot h)(a) + (g \cdot h)(a) = (f \cdot h + g \cdot h)(a) \end{aligned}$$

$$\begin{aligned} (f \cdot (g+h))(a) &= f((g+h)(a)) = f(g(a) + h(a)) = \\ &= f(g(a)) + f(h(a)) = (f \cdot g)(a) + (f \cdot h)(a) = \\ &= (f \cdot g + f \cdot h)(a) \end{aligned}$$

neutral:

$$\text{id}: A \rightarrow A, a \mapsto a$$

$$(f \cdot \text{id})(a) = f(\text{id}(a)) = \underline{f(a)} = \text{id}(f(a)) = (\text{id} \cdot f)(a)$$

$(\text{End } A, +, \cdot)$ ist Ring mit Eins, im allgemeinen nicht kommutativ

Speziell:

$$\text{End}(\mathbb{Z}, +) \cong (\mathbb{Z}, +, \cdot)$$

$$\varphi: \mathbb{Z} \rightarrow \text{End } \mathbb{Z}, n \mapsto (\mathbb{Z} \xrightarrow{\varphi_n} \mathbb{Z}, z \mapsto n \cdot z)$$

$$\begin{aligned} \varphi_n \text{ Endomorphismus: } \varphi_n(z+\tilde{z}) &= n \cdot (z+\tilde{z}) = n \cdot z + n \cdot \tilde{z} = \\ &= \varphi_n(z) + \varphi_n(\tilde{z}) \end{aligned}$$

Verträglichkeit mit der Addition:

$$\varphi(n+\tilde{n})(z) = \varphi_{n+\tilde{n}}(z) = (n+\tilde{n}) \cdot z = n \cdot z + \tilde{n} \cdot z = \varphi_n(z) + \varphi_{\tilde{n}}(z) = (\varphi_n + \varphi_{\tilde{n}})(z)$$

$$\varphi_{n \cdot \tilde{n}}(z) = n \cdot \tilde{n} \cdot z = n \cdot \varphi_{\tilde{n}}(z) = \varphi_n(\varphi_{\tilde{n}}(z)) = (\varphi_n \cdot \varphi_{\tilde{n}})(z)$$

$$\varphi_1 = \text{id}$$

injektiv: $\varphi_n = \varphi_{\tilde{n}} \Rightarrow n \cdot \varphi_n(1) = \varphi_{\tilde{n}}(1) = \tilde{n}$

surjektiv: $\varphi \in \text{End } \mathbb{Z} : \varphi = \varphi_{\varphi(1)} : \varphi(1 \cdot z) = \varphi(z) \stackrel{!}{=} \varphi_{\varphi(1)}(z) = \varphi(1) \cdot z$

Behauptung: $f = f(n)$

Induktion: $f(n) = f(1) \cdot n$ für $n \in \mathbb{N}$

J.A. $n=1$: $f(1) = f(1) \cdot 1$

J.S. $f(n+1) = f(n) + f(1) \stackrel{I.V.}{=} f(1) \cdot n + f(1) = f(1) \cdot (n+1)$

$$f(0) = 0 = f(1) \cdot 0$$

$$f(-n) + f(n) = f(0) = 0 = -f(n) + f(n)$$

$$\Rightarrow f(-n) = -f(n) = -f(1) \cdot n = f(1) \cdot (-n)$$

$$\text{End } \mathbb{Z}^2 \cong \mathbb{Z}^{2,2}$$

$$\mathbb{Z}^2 = \{ (z_1, z_2) \mid z_1, z_2 \in \mathbb{Z} \}$$

$$\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}$$

$$(z_1, z_2) + (\tilde{z}_1 + \tilde{z}_2) = (z_1 + \tilde{z}_1, z_2 + \tilde{z}_2) \quad \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

Zusätzliche Rechenregeln in einem Ring

$$0 \cdot a = 0 = a \cdot 0$$

$$0 + 0 \cdot a = 0a = (0+0)a = 0 \cdot a + 0a$$

$$a \cdot (-b) = -a \cdot b$$

$$(-a) \cdot (-b) = a \cdot b$$

Weiteres Beispiel: Der Polynomring $R[t]$ über einem kommutativen Ring in der Unbestimmten t .

Elemente: $a_0 + a_1 t + \dots + a_n t^n$, $a_j \in R$

$$\sum_{j=0}^n a_j t^j = \sum_{j=0}^{\infty} a_j t^j, \text{ fast alle } a_j = 0$$

Addition: $\sum_{j=0}^{\infty} a_j t^j + \sum_{j=0}^{\infty} \tilde{a}_j t^j = \sum_{j=0}^{\infty} (a_j + \tilde{a}_j) t^j$

Multiplikation: $\sum_{j=0}^{\infty} a_j t^j \cdot \sum_{k=0}^{\infty} b_k t^k = \sum_{l=0}^{\infty} \left(\sum_{j=0}^l a_j b_{l-j} \right) t^l$

$(\mathbb{R}[t], +)$ additive Gruppe (ohne Beweis)

Multiplikation assoziativ: $\left(\sum_{j=0}^{\infty} a_j t^j \cdot \sum_{k=0}^{\infty} b_k \cdot t^k\right) \cdot \sum_{r=0}^{\infty} c_r t^r =$

$$= \left(\sum_{l=0}^{\infty} \left(\sum_{j=0}^l a_j b_{l-j}\right) t^l\right) \cdot \sum_{r=0}^{\infty} c_r t^r = \sum_{s=0}^{\infty} \sum_{l=0}^s \left(\sum_{j=0}^l a_j b_{l-j} \cdot c_{s-l}\right) t^s =$$
$$= \sum_{j=0}^{\infty} a_j t^j \cdot \left(\sum_{k=0}^{\infty} b_k t^k \cdot \sum_{r=0}^{\infty} c_r t^r\right) = \left(\sum_{j=0}^{\infty} a_j t^j\right) \left(\sum_{q=0}^{\infty} \sum_{k=0}^q b_k c_{q-k} t^q\right) =$$
$$= \sum_{s=0}^{\infty} \sum_{j=0}^s a_j \cdot b_{s-j} \cdot c_s = \sum_{j=0}^{\infty} \sum_{j=0}^s \sum_{k=0}^{s-j} a_j b_k c_{s-j-k} t^s$$