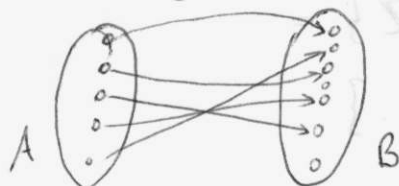


surjektiv, injektiv, bijektiv:

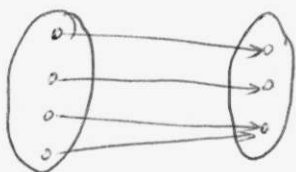
$$f: A \rightarrow B$$

injektiv:  $x, y \in A; x \neq y \Rightarrow f(x) \neq f(y)$

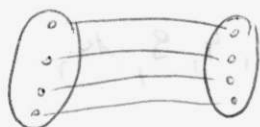


surjektiv:  $f: A \rightarrow B$

$$\forall x \in B: \exists y \in A; f(y) = x$$



bijektiv: injektiv + surjektiv



$f$  bijektiv  $\Rightarrow \exists f^{-1}$  (Umkehrung)

$$f \circ f^{-1} = f^{-1} \circ f = \text{id}_A$$

$$\text{id}_A(x) = x \quad \forall x \in A$$

$$A, B: |A| = |B| \Leftrightarrow \exists f: A \xrightarrow{1-1} B \text{ (bijektiv)}$$

Bsp.:  $\mathcal{P}(M); M \dots$  endlich

$$G(M) = \{A \subseteq M \mid |A| \text{ gerade}\}$$

$$U(M) = \{A \subseteq M \mid |A| \text{ ungerade}\}$$

$$x \in M; A \in G(M)$$

$$A \mapsto A \Delta \{x\}$$

$$\{x\} \in U(M)$$

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

$$m=5: \quad \mathbb{Z}_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$$

$$\begin{aligned} \bar{0} &= \{x \in \mathbb{Z} \mid x = 5 \cdot z; z \in \mathbb{Z}\} = \\ &= \{\dots, -10, -5, 0, 5, 10, \dots\} \end{aligned}$$

$$\begin{aligned} \bar{1} &= \{x \in \mathbb{Z} \mid x = 5 \cdot z + 1; z \in \mathbb{Z}\} = \\ &= \{\dots, -9, -4, 1, 6, 11, \dots\} \end{aligned}$$

$$\text{analog: } \bar{2}, \bar{3}, \bar{4}$$

$$\bar{3} + \bar{4} = \bar{2}; \quad \bar{1} + \bar{1} = \bar{2}$$

$$\bar{3} + \bar{4} = \bar{2}$$

$$\begin{aligned} \{\dots, -7, -2, 3, 8, 13, \dots\} + \{\dots, -6, -1, 4, 9, 14, \dots\} = \\ = \{\dots, -3, 2, 7, 12, \dots\} \end{aligned}$$

$$\begin{aligned} 5z+3 + 5l+4 &= 5(z+l)+3+4 = 5(\underbrace{z+l+1}_{\in \mathbb{Z}}) + 2 \\ z, l &\in \mathbb{Z} \end{aligned}$$

$$x \equiv y \pmod{m}$$

$$\rightarrow \exists \bar{z} \in \mathbb{Z}_m: x, y \in \bar{z}$$

$$\text{oder: } x - y = m \cdot l \quad l \in \mathbb{Z}$$

$$\text{oder: } x - y \equiv 0 \pmod{m}$$

$$\text{oder: } \bar{x} = \bar{y}$$

$$\mathbb{Z}_5: \quad \bar{2} \cdot \bar{3} = \bar{1} \quad ; z, l \in \mathbb{Z}$$

$$\begin{aligned} (5z+2)(5l+2) &= 25zl + 15z + 10l + 6 = \\ &= 5(\underbrace{5zl + 3z + 2l + 1}_{\in \mathbb{Z}}) + 1 \end{aligned}$$

$$a:b = \frac{a}{b} = a \cdot b^{-1}$$

$$\mathbb{Z}_5: \quad \bar{3}:\bar{4} = \bar{3} \cdot \bar{4}^{-1} = \bar{3} \cdot \bar{4} = \bar{2}$$

$$x \in \mathbb{Z}_5: \quad x \cdot \bar{4} = \bar{4} \cdot x = \bar{1}$$

$x$	$\bar{4} \cdot x$
$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{4}$
$\bar{2}$	$\bar{3}$
$\bar{3}$	$\bar{2}$
$\bar{4}$	$\bar{1}$

m... Primzahl:

$$\langle \mathbb{Z}_m, +, \cdot \rangle : \text{Körper}$$

$$\mathbb{Z}_6: \quad \bar{2}:\bar{3} = \bar{2} \cdot \bar{3}^{-1}$$

$$\bar{3} \cdot \bar{0} = \bar{0}$$

$$\bar{3} \cdot \bar{3} = \bar{3}$$

$$\bar{3} \cdot \bar{1} = \bar{3}$$

$$\bar{3} \cdot \bar{4} = \bar{0}$$

$$\bar{3} \cdot \bar{2} = \bar{0}$$

$$\bar{3} \cdot \bar{5} = \bar{3}$$

allgemein:  $\mathbb{Z}_m; \bar{a} \in \mathbb{Z}_m$

$$\text{ggT}(a, m) = 1 \Leftrightarrow \exists a^{-1}$$

in  $\mathbb{Z}_6$  kann nicht durch  $\bar{0}, \bar{2}, \bar{3}, \bar{4}$  dividiert werden  
 $\bar{5} \cdot \bar{5} = \bar{1}$  in  $\mathbb{Z}_6$  (Division durch  $\bar{5}$  möglich!)

$\langle M, \circ \rangle$  Monoid; abelsch?

$$a \circ b = b \circ a$$

Ring:  $\langle R, +, \cdot \rangle$ ;  $\langle R, + \rangle$  abelsche Gruppe  
~~SB für~~  $\langle R, \cdot \rangle$  Halbgruppe  
 Distributivgesetze

Körper:  $\langle K, +, \cdot \rangle$ ;  $\langle K \setminus \{0\}, \cdot \rangle$ : abelsche Gruppe

$$\Rightarrow \exists a \in K \Rightarrow 1 \cdot a = a \cdot 1 = a$$

$$\text{Multiplikation kommutativ} \Rightarrow 0 \cdot a = a \cdot 0 = 0$$

$$\langle \mathbb{Z}, +, \cdot \rangle \quad \exists z \in \mathbb{Z} \text{ mit } 2 \cdot z = z \cdot 2 = 1 !$$

$\Rightarrow$  kein Körper!

$$\langle \mathbb{Q}, +, \cdot \rangle : \quad \frac{a}{b} \cdot \frac{b}{a} = 1 \quad \Rightarrow \text{Körper}$$

$$\langle \underbrace{2 \cdot \mathbb{Z}}, +, \cdot \rangle \quad \exists a \in 2 \cdot \mathbb{Z} \text{ mit } e \cdot a = a \cdot e = 1$$

gerade ganze Zahlen

$\Rightarrow$  Ring

$$\{ f: K \rightarrow K \} :$$

$$(f+g)(u) = f(u) + g(u)$$

$$(f \circ g)(u) = f(g(u)) \quad ; \quad \text{nicht kommutativ, da } f \circ g \neq g \circ f$$

$\Rightarrow$  Ring

Ring:  $\langle R, +, \cdot \rangle$   $1, \langle R, + \rangle$  abelsche Gruppe  
 $R \neq \emptyset$  Einheits-element  $0$   
 inverses Element  $-a$

2,  $\langle R, \cdot \rangle$  Halbgruppe

3, distributive Gesetze  
 $a(b+c) = ab+ac$   
 $(b+c) \cdot a = ba+ca$

4,  $a \cdot 0 = 0 \cdot a = 0$

$\langle R, \cdot \rangle$  hat sogar Einheits-element  $\Rightarrow \langle R, \cdot \rangle$  Monoid  
 Annahme:  $R = \{0\}$  (Nullring, Zeroring)

„Normalfall“:

In jedem Ring gilt  $0 \cdot a = a \cdot 0 = 0$  f.  $a \in R$

Einheits-element der Multiplikation ist  $e \neq 0$ ,  
 falls  $|R| \geq 2$

wäre  $e = 0$ :

$$e \cdot a = a \cdot e = a \text{ f. } a \in R$$

und  $e \cdot a = a \cdot e = e = 0$  f.  $a \in R \Rightarrow a = 0!$

$\Rightarrow$  Ring mit Einselement

$\langle R, \cdot \rangle \rightarrow \langle R \setminus \{0\}, \cdot \rangle$  (kein inverses Element für 0)

Wann ist  $\langle R \setminus \{0\}, \cdot \rangle$  kein Gruppoid?

(R ist nicht der Zeroring)

Wenn Elemente  $a, b \in R$  existieren ( $a, b \neq 0$ ),  
 sodass  $a \cdot b = 0$ .

Bsp.: Restklassen  $\mathbb{Z}_6$

$$\overline{2} \cdot \overline{3} = \overline{6} = \overline{0}$$

Definition:  $a \in R$  heißt Nullteiler in  $R$ , wenn

1,  $a \neq 0$

2, es existiert  $b \in R, b \neq 0$ , sodass entweder  $a \cdot b = 0$  oder  $b \cdot a = 0$ .

Kommutativer Ring mit Einselement, aber ohne Nullteiler, d.h.  $\langle R, \setminus \{0\}, \cdot \rangle$  ist abgeschlossen, heißt Integritätsbereich.

Integritätsbereich:  $\langle R, +, \cdot \rangle$

1,  $\langle R, + \rangle$  abelsche Gruppe (Einheitselement 0)

2,  $\langle R_0, \cdot \rangle$  abelsches Monoid

$$(R_0 = R \setminus \{0\})$$

3,  $a \cdot 0 = 0 \cdot a = 0$  f. a.  $a \in R$

4, Distributivgesetz:

$$\begin{array}{l} \top a(b+c) = ab+ac \quad \top \\ \bot (b+c) \cdot a = ba+ca \quad \bot \end{array}$$

Körper:  $\langle K, +, \cdot \rangle$

1,  $\langle K, + \rangle$  abelsche Gruppe (Einheitselement 0)

2,  $\langle K \setminus \{0\}, \cdot \rangle$  abelsche Gruppe

3,  $a \cdot 0 = 0 \cdot a = 0$  f. a.  $a \in R$

4, Distributivgesetz

Es gilt (Satz von Wedderburn): jeder endliche Integritätsbereich ist ein Körper

Bemerkung: Schiefkörper: Multiplikation ist nicht (notwendigerweise) kommutativ

Halbring:  $\langle R, +, \cdot \rangle$

1,  $\langle R, + \rangle$  Halbgruppe (meist kommutativ, oft Monoid)

2,  $\langle R, \cdot \rangle$  Halbgruppe

3, Distributivgesetze

Satz von Wedderburn:

Einheitselement bezüglich Multiplikation: 1

	$a_1$	$\dots$	$a_n$
$a_1$			
$\vdots$			
$\vdots$			
$a = a_j$			

existiert  $a'$ , sodass  $a \cdot a' = 1$

$a'$  existiert genau dann, wenn in der Zeile " $a$ " 1 vorkommt.

angenommen, 1 kommt nicht vor unter  $n$  Elementen der Zeile " $a$ "  $b_1 \dots b_n$

$\Rightarrow$  es mssen zwei Elemente gleich sein (1 kommt nicht vor!):  $b_i = b_k \quad i \neq k$

$$b_i = a \cdot a_i$$

$$b_k = a \cdot a_k$$

$$i \neq k \Rightarrow a_i \neq a_k$$

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

$$a(a_i + a_k) = 0$$

Integrittsbereich:  $a \neq 0$

$$\Rightarrow a_i + (-a_k) = 0$$

$$a_i = a_k$$

$\Rightarrow$  WIDERSPRUCH!

Bsp. 88:

$$\langle \mathbb{Z}_3, + \rangle \times \langle \mathbb{Z}_2, + \rangle = \langle G, \oplus \rangle$$

$$\mathbb{Z}_3 \times \mathbb{Z}_2$$

$$\langle \mathbb{Z}_3, \oplus_3 \rangle \times \langle \mathbb{Z}_2, \oplus_2 \rangle$$

$$\langle a_1, b_1 \rangle \oplus \langle a_2, b_2 \rangle =$$

$$= \langle a_1 \oplus a_2, b_1 \oplus b_2 \rangle$$

$$\langle \mathbb{Z}_3, \oplus_3 \rangle$$

$\oplus_3$	0	1	2
0	0	1	2
1	2	0	1
2	1	2	0

$y+y (=2y)$

$$\langle \mathbb{Z}_2, \oplus_2 \rangle$$

$\oplus_2$	0	1
0	0	1
1	1	0

$z+z (=2z)$

$$\langle 1, 1 \rangle + 2x = \langle 2, 1 \rangle$$

$$x = \langle y, z \rangle$$

$$2x = x + x = \langle y+y, z+z \rangle$$

$$\langle 1, 1 \rangle + \langle y+y, z+z \rangle = \langle 2, 1 \rangle$$

$$\langle 1+y+y, 1+z+z \rangle = \langle 2, 1 \rangle$$

Gesucht  $y$ :

$$1 + \underbrace{y+y}_{2y} = 2$$

$$1 + 2y = 2$$

$$1 + 1 = 2$$

$$\text{Gesucht } y: 2y = 1 \Rightarrow \underline{y = 2}$$

Gesucht  $z$ :

$$1 + \underbrace{z+z}_{2z} = 1$$

$$1 + 2z = 1$$

$$1 + 0 = 1$$

$$\text{Gesucht } z: 2z = 0$$

2 Lösungen:  $\underline{z=0}$  und  $\underline{z=1}$

$$\Rightarrow \underline{x = \langle 2, 0 \rangle} \quad \text{und} \quad \underline{x = \langle 2, 1 \rangle}$$



MAR

12.11.2004

$$(\lambda \cdot a + \lambda \cdot o) = \lambda \cdot (a + o) = \lambda \cdot a$$

$$-\underbrace{\lambda \cdot a}_{o} + \lambda \cdot a - \lambda \cdot o = \underbrace{\lambda \cdot a - \lambda \cdot a}_{o}$$

$$\underbrace{o + \lambda \cdot o}_{o} = o$$

$$\underline{\lambda \cdot o = o}$$

$A: U \rightarrow V$  (lineare Abbildung)

$$\text{Ker } A = \{v \mid v \in U; A(v) = 0_v\}$$

Bsp.:  $U = K^p \quad V = K^1$

lineares Funktional:  $A(v) = x_1 + x_2 + \dots + x_p$

$$\text{Ker } A = \{v \mid x_1 + x_2 + \dots + x_p = 0\} =$$

$$= \left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_{p-1} \\ -\sum_{j=1}^{p-1} x_j \end{pmatrix} \mid x_1, \dots, x_{p-1} \in K \right\}$$

$A: U \rightarrow V$ ;  $\text{Ker } A$ ;  $y \in V^*$ ;  $y \in A(U)$

Gesucht:  $T = \{v \mid v \in U; A(v) = y\}$

$$v_1, v_2 \in T$$

$$A(v_1) = A(v_2) = y \Rightarrow v_1 - v_2 \in \text{Ker } A$$

$$\underbrace{A(v_1) - A(v_2)} = y - y = 0$$

$$A(v_1 - v_2) = 0$$

Es existiert  $z \in \text{Ker } A$ , sodass  $v_1 - v_2 = z$

$$v_1 = v_2 + z$$

d.h. gibt  $A(v_0) = y$  für ein „bestimmtes“  $v_0 \in U$ ,  
 es existiert für jedes andere  $v$  mit  $A(v) = y$   
 ein  $z \in \text{Ker } A$  mit  $v = v_0 + z$

d.h.  $v \in v_0 + \text{Ker } A$

also  $T \subseteq v_0 + \text{Ker } A$

Sei  $x \in x_0 + \ker A$

D. h. es existiert  $z \in \ker A$ , sodass  $x = x_0 + z$ ,

$$\text{dann gilt } A(x) = A(x_0 + z) = A(x_0) + A(z) = \\ = y + 0 = y$$

d. h.  $y \in T$

somit  $x_0 + \ker A \subseteq T$

also:  $T = x_0 + \ker A$

---

System  $S$  l. u.

$\{a_1, \dots, a_p\}$  l. u.

$\Rightarrow b_1, \dots, b_n \in S$

$\{b_1, \dots, b_n\}$  l. u.

$$\lambda_1 b_1 + \lambda_2 b_2 + \dots + \lambda_n b_n = 0 \Rightarrow \lambda_1 = 0; \lambda_2 = 0; \dots; \lambda_n = 0$$

$$\mu_1 a_1 + \dots + \mu_p a_p = r \Rightarrow \mu_1 = 0; \dots; \mu_p = 0$$

Def.  $a_1, \dots, a_j$

$$S_j = (S \setminus \{b_1, \dots, b_j\}) \cup \{a_1, \dots, a_j\}$$

$a_{j+1} = r$ , weil  $a_j \in \{a_1, \dots, a_p\}$  l. u.

also existiert  $v \in S_j$ , sodass  $\underbrace{(S_j \setminus \{v\}) \cup \{a_{j+1}\}}_{S_{j+1}} \text{ l. u.}$

Behauptung:  $v$  ist wählbar, dann  $v \notin \{a_1, \dots, a_j\}$

d.h.  $v \in S$  wählbar

Beweis:  $a_{j+1}$  da  $S_j$  Basis:

$$a_{j+1} = \sum_{k=1}^m \mu_k v_k \quad v_k \in S_j$$

nicht alle  $\mu_k = 0$

daher o. B. d. A. alle  $\mu_k \neq 0$ ; trotzdem  $m \geq 1$ ,

da  $a_{j+1} \neq 0$   
 $a_{j+1}$  ist gegen jeden dieser  $v_1, \dots, v_m$  austauschbar

Behauptung:  $\{v_1, \dots, v_m\} \not\subseteq \{a_1, \dots, a_j\}$

Beweis indirekt:

Angenommen  $\{v_1, \dots, v_m\} \subseteq \{a_1, \dots, a_j\}$

$a_{j+1} : \{v_1, \dots, v_m, a_{j+1}\} \subseteq \{a_1, \dots, a_j, a_{j+1}\}$

Wenn keine Menge (da System):

$a_{j+1} = v_k$ ; dann  $v_k \in \{a_1, \dots, a_j\}$

$\Rightarrow m=1$   $a_{j+1} = v_1$

d.h.  $a_{j+1} \in \{a_1, \dots, a_j\}$   
 Widerspruch!

$$\begin{aligned} \text{l.u.} \{v_1, \dots, v_m, \alpha_{j+1}\} &\subseteq \{\alpha_1, \dots, \alpha_j, \alpha_{j+1}\} \\ \text{Menge} &\subseteq \underbrace{\{\alpha_1, \dots, \alpha_p\}}_{\text{l.u.}} \end{aligned}$$

$$\text{aber: } \sum_{k=1}^m \mu_k v_k + \underbrace{(-1)\alpha}_{\substack{\uparrow \\ \neq 0}} = 0$$

nicht-triviale Linearkombination

also  $\{v_1, \dots, v_m, \alpha_{j+1}\}$  l.a. ! Widerspruch!