§ 1 Rechenregeln: Ringe, Körper, Anordnung

In diesem Kapitel geht es um Zahlen und ihre Rechenregeln, die Sie aus der (Grund-) Schule kennen. Wir betrachten sie aber etwas genauer und mathematischer.

1. Def Gegeben sei eine Menge R (zum Beispiel die Menge $\mathbb{Z}$ der ganzen Zahlen, $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \dots\}$.

In R soll es zwei besondere Elemente geben, die wir 0 und 1 nennen, also $0, 1 \in R$. [lies: 0,1 sind Elemente von R]

Weiter soll es auf R zwei Verknüpfungen

$+$ und $\cdot$ sehen, die zwei beliebigen Elementen $x, y \in R$ jeweils neue Elemente $x+y \in R$ und $x \cdot y \in R$ zuordnen. Wir nennen $(R, +, \cdot, 0, 1)$ einen (kommutativen) Ring, wenn für alle $x, y, z \in R$ folgende Regeln gelten.

(K_+) $x+y = y+x$
$(K_\cdot)$ $x \cdot y = y \cdot x$
} Kommutativ-Gesetze

(A_+) $(x+y)+z = x+(y+z)$
$(A_\cdot)$ $(x \cdot y) \cdot z = x \cdot (y \cdot z)$
} Assoziativ-Gesetze

Die Klammern sehen die Reihenfolge der Ausführung der Verknüpfungen an.

(D) $x \cdot (y+z) = (x \cdot y) + (x \cdot z)$
$(x+y) \cdot z = (x \cdot z) + (y \cdot z)$
} Distributiv-Gesetz

(N_1) $x \cdot 1 = 1 \cdot x = x$
(N_0) $x + 0 = 0 + x = x$
} Neutralelemente

(I_+) Zu jeden x gibt es genau ein y mit $x + y = 0$

Schreibe dann $y = -x$.

Diese Rechenregeln kennen wir aus der Schule. Sie gelten für die ganzen Zahlen, die rationalen Zahlen und die reellen Zahlen.

Dagegen gilt sie nicht für die natürlich Zahl $\mathbb{N} = \{0,1,2,3,\dots\}$, es gibt keine natürlich Zahl n mit

$n+1 = 0$ (-1 ist keine natürlich Zahl)

2. Ein Beispiel aus der Informatik.

Betrachte $\mathbb{F}_2 = \{0,1\}$ mit folgenden Verknüpfungen

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

Man kann nachrechnen, dass $(\mathbb{F}_2, +, \cdot, 0, 1)$ ein Ring ist.

Beachte: in $\mathbb{F}_2$ gilt stets $x+x=0$

also $x = -x$ für alle $x \in F_2$ (!)

3. Aus den Rechenregeln eines Ringes folgen leicht weitere Regeln.
Nach (A_+), $(A_\cdot)$ können wir viele Klammern weglassen. Wir verwenden auch immer die Schreibweise "Punktrechnung vor Strichrechnung", also

$$x \cdot y + z = (x \cdot y) + z \quad \text{usw}$$
$$x + (-y) = x - y$$

Weitere Rechenregeln folgen. #

- $-(-x) = x$
  denn: $-x + (-(-x)) = 0$

- aus $x + y = x$ folgt $y = 0$ ("Kürzen bei Addition")

  denn: $0 = x + y - x = x - x + y = y$

- $0 \cdot x = x \cdot 0 = 0$

  denn: $0 \cdot x = (0+0) \cdot x = 0 \cdot x + 0 \cdot x$

  $\Rightarrow 0 = 0 \cdot x$ genauso $0 = x \cdot 0$

- $(-x) \cdot y = -(x \cdot y)$

  denn: $x \cdot y + (-x) \cdot y = (x - x) \cdot y = 0 \cdot y = 0$

  $\Rightarrow (-x) \cdot y = -(x \cdot y)$

- Insbesondere gilt $(-1) \cdot x = -x$

  und $(-x) \cdot (-y) = x \cdot y$

u.v.a.

Beachte: unsere kleine Beweise gelten in jedem Ring, nicht nur in den aus der Schule vertrauten Zahlen! Sie gelten also auch in $\mathbb{F}_2$.

Somit kann kein Teilen / Division vor.

4. Def Ein Ring $(R, +, \cdot, 0, 1)$ heißt

Körper, wenn gilt

$0 \neq 1$ (das hatten wir bisher nicht explizit verlangt)

und

(I_0) Ist $x \in R$ mit $x \neq 0$, so gibt es genau ein $y \in R$ mit $x \cdot y = y \cdot x = 1$.

Schreibe dann kurz $y = x^{-1} = \frac{1}{x}$.

Beispiele: • Die rationalen Zahlen

$$\mathbb{Q} = \underbrace{\left\{ \frac{a}{b} \mid a, b \in \mathbb{Z}, \; b \neq 0 \right\}}_{\text{ganzzahlige Brüche}}$$

bilden ein Körper, ebenso die reellen Zahlen $\mathbb{R}$.

• Die ganzen Zahlen $\mathbb{Z}$ bilden kein Körper, da gibt kein ganze Zahl m

mit $m \cdot 2 = 1$ (denn $\frac{1}{2}$ ist keine ganze Zahl)

- $\mathbb{F}_2$ ist ein Körper.

Die ganzen / rationalen / reellen Zahlen können wir der Größe nach vergleichen, über ihre Anordnung.

5. Def (a) Sei X eine Menge und sei $<$ eine zweistellige Relation auf X (d.h. für $x, y \in X$ gilt entweder $x < y$ oder nicht $x < y$, schreib dann $x \not< y$.

Wir nennen $<$ eine Anordnung oder totale Ordnung, falls für alle $x, y, z \in X$ gilt

(A1) es gilt nie $x < x$

(A2) ist $x \neq y$, so gilt entweder $x < y$ oder $y < x$

(A3) ist $x < y$ und $y < z$, so gilt $x < z$.

(b) Sei R ein Ring mit $0 \neq 1$ und sei $<$ eine Anordnung auf der Menge R. Wir nennen $(R, +, \cdot, 0, 1, <)$ einen angeordneten Ring, wenn für alle $x, y, z \in R$ gilt

(AR1) wenn $x<y$, dann $x+z<y+z$

(AR2) wenn $x<y$ und $0<z$, dann $x\cdot z<y\cdot z$

Konventionen $y>x$ heißt $x<y$

$x\leq y$ heißt $x<y$ oder $x=y$

Wir nennen x positiv, wenn $x>0$ und negativ, wenn $x<0$.

Konsequenzen

(1) $x,y>0 \Rightarrow x\cdot y>0$

(mit AR2)

(2) $x<0 \Leftrightarrow -x>0$

denn: $x<0 \overset{(AR1)}{\Rightarrow} x-x<0-x$ d.h. $0<-x$

$0<-x \overset{(AR1)}{\Rightarrow} x<x-x=0$

(3) $x,y<0 \Rightarrow x\cdot y>0$

denn: $x,y<0 \Rightarrow -x,-y>0 \Rightarrow \underbrace{(-x)(-y)}_{=x\cdot y}>0$

↑

§1,3

(4) $x<0<y \Rightarrow x\cdot y<0$

denn $x<0 \overset{(AR2)}{\Rightarrow} xy<0\cdot y=0$

(5) $x \neq 0 \Rightarrow x^2 > 0$

denn: $x > 0$ oder $x < 0$, beide (1) oder (3).

Insbesondere ist $1 = 1 \cdot 1 > 0$ (denn wir haben angenommen, dass $1 \neq 0$!)

(6) Es folgt

$0 < 1 < 1+1 < 1+1+1 < \ldots$

also hat R unendlich viele Elemente.

Wir haben bewiesen: jeder angeordnete Ring ist unendlich.

6. Def Es sei R ein angeordneter Ring oder Körper, zum Beispiel $R = \mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \ldots\}$

Für $x \in R$ definieren wir den Absolutbetrag

$$|x| = \begin{cases} x & \text{falls } x \geq 0 \\ -x & \text{falls } x < 0 \end{cases}$$

Dann gilt für alle $x, y \in R$ folgendes

(1) $|x \cdot y| = |x| \cdot |y|$

(2) $|x| = |-x| \geq 0$

(3) $|x+y| \leq |x| + |y|$ (Dreiecksungleichung)

(4) $||x|-|y|| \leq |x-y|$ (umgekehrte Dreiecksungleichung)

Beweis (1) Durch Fallunterscheidung

$x, y > 0 \Rightarrow |x| = x \,,\; |y| = y \Rightarrow |x \cdot y| = xy = |x| \cdot |y|$

$x = 0 \Rightarrow xy = 0$

$x, y < 0 \Rightarrow |x| = -x \quad |y| = -y \quad |x \cdot y| = xy = (-x)(-y) = |x| \cdot |y|$

$x < 0 < y \Rightarrow |x| = -x \quad |y| = y \quad |xy| = -xy = (-x)y = |x| \cdot |y|$

(2) $x \geq 0 \Rightarrow |x| = x \Rightarrow |x| \geq 0$

$x < 0 \Rightarrow |x| = -x > 0$ und $|x| = |-x|$

(3) Voraussetzung: $|x| \geq \pm x \quad |y| \geq \pm y$ nach (2)

$|x| + |y| \geq |x| + y \geq x + y$

$|x| + |y| \geq |x| - y \geq -x - y \overset{(!)}{=} -(x+y)$

also $|x| + |y| \geq \pm (x+y)$

$\Rightarrow |x| + |y| \geq |x+y|$

(4) $|x| = |x - y + y| \overset{(2)}{\leq} |x-y| + |y|$

$|y| = |x - x + y| \leq |x| + |-x+y| = |x| + |x-y|$

ab. $|x| - |y| \leq |x-y|$

$|y| - |x| \leq |x-y|$

$\Rightarrow \big||x| - |y|\big| \leq |x-y|$

□

7. Die natürlichen Zahlen $\mathbb{N} = \{0, 1, 2, 3, \dots\}$

Was sind die natürlichen Zahlen? Diese Frage haben wir bisher nicht gestellt.

- Beobachtungen über $\mathbb{N}$

(1) Jede natürliche Zahl n hat einen Nachfolger $n+1$, die kleinste natürliche Zahl, die größer als n ist

(2) 0 ist kein Nachfolger

(3) jede natürliche Zahl $n \neq 0$ ist ein (n-ter) Nachfolger von 0
"jede natürliche Zahl erhält man durch zählen ab 0"

8. Definition (Die Peano-Axiome)

↑ italienischer Mathematiker

Eine Nachfolgerstruktur $(N, s, 0)$ besteht aus einer Menge N, einem Element $0 \in N$ und einer Abbildung s, die jedem $n \in N$ ein Element $s(n)$ zuordnet. Dabei soll folgendes gelten.

(P1) Es gibt kein $n \in N$ mit $s(n) = 0$

(P2) Wenn $s(n) = s(m)$, so $n = m$
("s ist injektiv")

(P3) Ist M eine Teilmenge von $\mathbb{N}$ ("$M \subseteq \mathbb{N}$") und gilt

(a) $0 \in M$

(b) wenn $n \in M$, dann $s(n) \in M$

("M ist abgeschlossen")

dann ist $M = \mathbb{N}$

Das sind die Peano-Axiome der natürlichen Zahlen.

9. Beispiel $N = \mathbb{N}$, $o = 0$, $s(n) = n+1$.

Man kann folgendes beweisen. Ist (N, s, o) eine Nachfolgerstruktur, so gibt es genau eine Abbildung $f: \mathbb{N} \to N$ mit folgenden Eigenschaften

(a) $f(0) = o$

(b) $f(k+1) = s(f(k))$

(c) $f(k) = f(l) \Rightarrow k = l$
(f ist injektiv)

(d) zu jedem $n \in N$ gibt es ein $k \in \mathbb{N}$ mit $f(k) = n$
(f ist surjektiv)

Die Peano-Axiome kennzeichnen also die natürlichen Zahlen eindeutig.

Man kann Addition und Multiplikation rekursiv definieren durch:

$$0 + n = 0 \qquad\qquad 0 \cdot n = 0$$

$$S(m) + n = S(m+n) \qquad\qquad S(m) \cdot n = m \cdot n + n$$

Dann kann (und muss) man beweisen, dass die Kommutativ-, Assoziativ- und Distributivgesetze gelten. Wir tun das hier nicht.

10. Peanos Axiom (P3) ist das <u>Prinzip der Induktion</u>. Wir formulieren es noch einmal für $\mathbb{N}$:

(P3) Ist $M \subseteq \mathbb{N}$ eine Menge von natürlichen Zahlen und gilt

(a) $0 \in M$

(b) für jedes $m \in M$ ist auch $m+1 \in M$

dann ist $M = \mathbb{N}$

Ein Beispiel

Beh: Es gilt für alle $n \in \mathbb{N}$ die Formel

$$0+1+2+3+\ldots+n = \frac{n(n+1)}{2}$$

Beweis mit (P3) d.h. mit Induktion

Set $M = \{ m \in \mathbb{N} \mid$ die Formel stimmt für $m \}$

Induktionsanfang

Für $m = 0$ ist $0 = \frac{m(m+1)}{2}$ (✓)

(d.h. $0 \in M$)

Induktionsschritt

Wenn die Formel für m gilt, dann gilt sie auch für $m+1$.

(d.h. $m \in M \Rightarrow m+1 \in M$)

Denn

$$0+1+\ldots+m = \frac{m(m+1)}{2} \qquad \text{addiere } (m+1)$$

$$0+1+\ldots+m+(m+1) = \frac{m(m+1)}{2} + (m+1)$$

$$= \frac{m(m+1)}{2} + \frac{2(m+1)}{2}$$

$$= \frac{(m+2)(m+1)}{2} \qquad (\checkmark)$$

Mit (P3) folgt: die Formel gilt für alle $m \in \mathbb{N}$, denn $\mathbb{N} = M$.

II. Die Anordnung von $\mathbb{N}$

Wir definieren eine (zweistellige) Relation $\leq$ auf $\mathbb{N}$ wie folgt.

$m \leq n \overset{\text{DEF}}{\iff}$ es gibt $l \in \mathbb{N}$ mit $m + l = n$

$m < n \overset{\text{DEF}}{\iff} m \leq n$ und $m \neq n$

Satz Damit ist $<$ eine Anordnung auf $\mathbb{N}$.

Beweis in 3 Schritten.

(1) Für alle m, n gilt $m \leq n$ oder $n \leq m$.

Denn: setze $M = \{ m \in \mathbb{N} \mid$ für alle $n \in \mathbb{N}$ gilt $m \leq n$ oder $n \leq m \}$

dann ist $0 \in M$ ($0 + n = n \Rightarrow 0 \leq n$)

Sei $m \in M$, zeige $m + 1 \in M$

Für $n \in \mathbb{N}$ gibt es die Möglichkeiten

(a) $n \leq m$, also $n + l = m$

$\Rightarrow n + l + 1 = m + 1 \Rightarrow n \leq m + 1$

(b) $m < n$, also $m + l = n$ und $l \neq 0$

* Bemerkung: Jede natürliche Zahl $n \neq 0$ ist ein Nachfolger.

Beweis Sei $M = \{0\} \cup \{n \in \mathbb{N} \mid n \text{ ist Nachfolger}\}$

Dann gilt $0 \in M$. Ist $m \in M$, so folgt $s(m) = m+1 \in M$, denn $m+1$ ist Nachfolger.

Nach (P3) ist $M = \mathbb{N}$. □

$\Rightarrow \quad l = k+1 \quad$ für ein k

$m + k+1 = n \quad \Rightarrow \quad (m+1) \leq n$

Es folgt $M = \mathbb{N}$ (mit P3) ∎

2. Ist $m \leq n$ und $n \leq m$, so ist $m = n$

Denn: $m + l = n \qquad n + k = m \quad \Rightarrow \quad m + k + l = m$

Beh A Sind $x, y \in \mathbb{N}$ mit $x + y = x$, so ist $y = 0$

Das stimmt für $x = 0$, jetzt Induktion

$(x+1) + y = x + 1 \overset{(P2)}{\Rightarrow} x + y = x \Rightarrow y = 0$

Beh B Sind $x, y \in \mathbb{N}$ mit $x + y = 0$, so ist $x = y = 0$

Das stimmt für $x = 0$. Angenom, $x = z + 1$.

$\Rightarrow (z+1) + y = 0 \Rightarrow 0$ ist Nachfolger ↯

ein Widerspruch zu (P1)

Insgesamt folgt $k + l = 0$ und damit $k = l = 0$.

Damit ist (A2) aus §1.5 gezeigt.

3. Ist $l < m$ und $m < n$, so ist $l < n$.

$$\left.\begin{aligned} l + r &= m \qquad r \neq 0 \\ m + s &= n \qquad s \neq 0 \end{aligned}\right\} \Rightarrow l + (r+s) = n$$

und $r + s \neq 0$, also $l < n$

Damit gilt (A3) □

Das Induktionsprinzip hat zwei wichtige Varianten.

12. Das Wohlordnungsprinzip

Satz Sei $S \subseteq \mathbb{N}$ eine beliebige, nicht leere Menge von Zahlen, $S \neq \emptyset$. Dann enthält S genau ein kleinstes Element $s \in S$, d.h. $s \leq m$ für alle $m \in S$. Wir schreiben

$$s = \min(S)$$

Beweis Sei $M = \{ m \in \mathbb{N} \mid \text{für alle } t \in S \text{ ist } m \leq t \}$

Dann gilt $0 \in M$, denn $0 \leq t$ gilt für alle $t \in S$.

Wenn $t \in S$, so ist $t+1 \notin M$, denn $t+1 \not\leq t$. Folglich ist $M \neq \mathbb{N}$ (denn S ist nicht leer). Nach dem Induktionsprinzip muss es $s \in M$ geben mit $s+1 \notin M$. Für alle $t \in S$ ist dann $s \leq t$.

Beh $s \in S$.

Dann wenn $s \notin S$, so wäre $s < t$ für alle $t \in S$. Aber dann wäre $s+1 \leq t$ für alle $t \in S$, also $s+1 \in M$ ↯

Damit ist $s \in S$.

Ist $s' \in S$ ein anderes kleinstes Element in S, so folgt $s \leq s'$ und $s' \leq s$, also $s = s'$. □

13. Das 2. Induktionsprinzip

Es sei $M \subseteq \mathbb{N}$ eine Teilmenge mit folgender Eigenschaft: Für jedes $n \in \mathbb{N}$

wenn für alle natürlichen Zahlen $m \in \mathbb{N}$ mit $m < n$ gilt $m \in M$, dann ist auch $n \in M$.

Dann ist $M = \mathbb{N}$.

Beweis: $n = 0$ muss für alle $m < n$ gilt $m \in M$, denn es gibt gar kein $m < n$ (!).

Angenommen, $M \neq \mathbb{N}$. Sei $n \in \mathbb{N}$ die kleinste natürliche Zahl, die nicht in

M hat. (Das gibt es dann nach dem Wohlordnungsprinzip). Für alle $m < n$ ist dann $m \in M$. Also dann gilt nach Annahme $n \in M$ ↯. Also ist $M = \mathbb{N}$. □

14. Exkurs über Mengen

Der Begriff der Menge ist zentral in der Mathematik, denn alle dort betrachteten Dinge und Strukturen sind Mengen. Die Vorstellung einer Menge ist, bestimmte Dinge zusammenzufassen.

Die grundlegende Beziehung zwischen Menge ist:

$x \in A$ "x ist ein Element der Menge A"

$x \notin A$ "x ist kein Element der Menge A"

Die Menge B heißt Teilmenge der Menge A, wenn jedes Element von B auch Element von A ist.

Schreibe dafür:

$B \subseteq A$ heißt: "für alle $x \in B$ gilt auch $x \in A$".

Der Begriff der Menge hat sich im 19. Jahrhundert entwickelt. Es gibt einige Spielregeln, wie Mengen gebildet werden, die wir jetzt durchgehen.

(Ex) es gibt die <u>leere Menge</u> $\emptyset$, deren Kennzeichen es ist, <u>keine</u> Elemente zu haben

(Ext) zwei Mengen A, B sind genau dann gleich, wenn sie die gleichen Elemente haben,

$A = B$ genau dann, wenn $A \subseteq B$ <u>und</u> $B \subseteq A$ gilt.

Mengen werden ausschließlich durch ihre Elemente bestimmt.

(Aus) Ist X eine Menge und $\varphi(a)$ eine Bedingung an a, die wahr oder falsch sein kann (ab hängig von a), so ist

$\{ a \in X \mid \varphi(a) \text{ ist wahr} \}$ eine Menge

Beispiel $X = \mathbb{N}$ $H = \{ a \in \mathbb{N} \mid a \text{ ist gerade} \}$

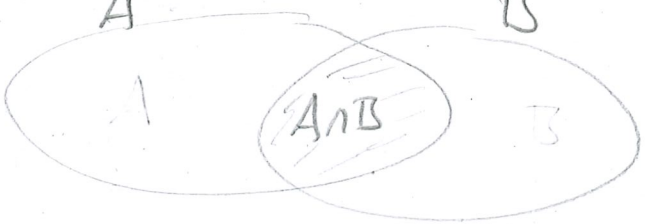
ist eine Teilmenge von $\mathbb{N}$, die Menge der geraden natürlichen Zahlen.

Beispiel $\phi = \{\} = \{ a \in \mathbb{N} \mid a \neq a \}$

Beispiel A, B Mengen. Dann ist ihr

Durchschnitt $A \cap B = \{ a \in A \mid a \in B \}$

$= B \cap A$



Wenn ist $A \cap B = \phi$, so heißen A und B disjunkt.

Bsp A, B Mengen

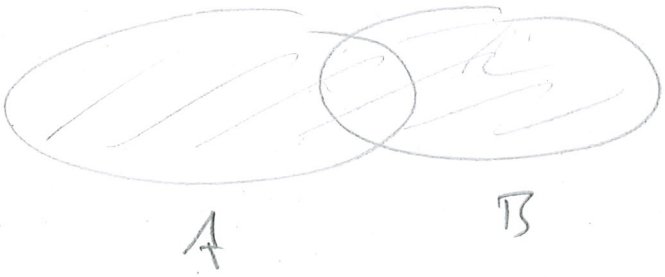
$A - B = A \setminus B = \{ a \in A \mid a \notin B \}$

Das Komplement von B in A.

(Paar) Wenn a, b Mengen sind, so ist $A = \{a, b\}$ eine Menge, mit a, b als einzigen Elementen. Allgemein für $a_1, a_2, \ldots, a_m$

$$A = \{a_1, a_2, \ldots, a_m\}.$$

(Ver) Sind A, B Mengen, so ist auch die Vereinigung $A \cup B = \{x \mid x \in A \text{ oder } x \in B\}$ eine Menge



Ist X eine Menge, so ist

$$\bigcup X = \{x \mid \text{es gibt } a \in X \text{ mit } x \in a\}$$

die Vereinigung der in X enthaltenen Mengen,

Bsp $\bigcup \{A, B\} = A \cup B$

(Pot) Ist A eine Menge, so ist ihre Potenzmenge $P(A) = \{B \mid B \subseteq A\}$

eine Menge, die Elemente von $P(A)$ sind genau die Teilmengen von A.

(Inf) Es gibt unendliche Mengen.

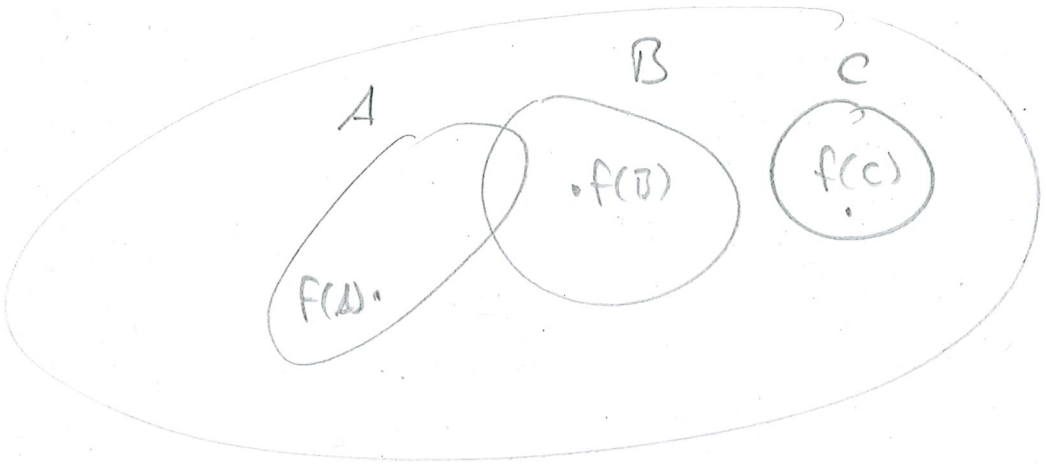
Genauer: sehe $s(a) = a \cup \{a\}$.
Es gibt eine Menge N, die nicht leer ist, mit der Eigenschaft:
wenn $a \in N$ gilt, so auch $s(a) \in N$.
$\rightarrow$ Zahlen (später)

(Fund) Wenn $X \neq \emptyset$ eine Menge ist, so gibt es $a \in X$ mit $a \cap X = \emptyset$.

Folgerung Es gilt niemals $A \in A$.

Denn Angenommen, $A \in A$. Sei $X = \{A\}$, es folgt $A \cap \{A\} = \emptyset$. Aber $A \in A$ und $A \in \{A\}$ $\lightning$ ein Widerspruch.

(Aus) Ist X eine Menge von nichtleeren Mengen, dann gibt es eine Abbildung f, die jedem $A \in X$ ein Element $f(A) \in A$ zuordnet



Die Notwendigkeit, Mengen nach bestimmten Regeln zu betrachten, wurde nötig durch Russels Antinomie: angenommen, wir dürfen solch

$$R = \{ x \mid x \notin x \}$$

wenn $R \notin R \Rightarrow R \in R$ ↯
wenn $R \in R \Rightarrow R \notin R$ ↯
Nach den obigen Regeln gibt es keine solche Menge R.

15. Paare, Tupel, kartesisch Produkte

Idee ein geordnetes Paar (x,y) hat einen erste Eintrag x und ein zweite Eintrag y.

Es gilt $(x,y) = (u,v)$ genau dann, wenn $x = u$, $y = v$

(aber $(x,y) \neq \{x,y\}$!)

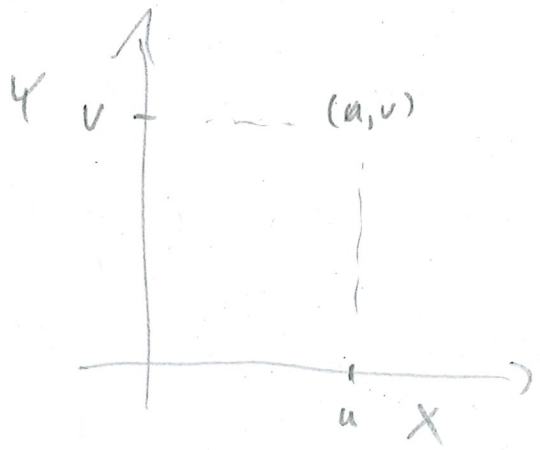
(Man kann (x,y) als Menge wie folgt kodieren

$(x,y) = \{\{x\}, \{x,y\}\}$

$\{\{u\},\{u,v\}\} = \{\{x\},\{x,y\}\}$ gdw $u = x$, $v = y$)

Das kartesische Produkt der Mengen X, Y ist

$$X \times Y = \{ (u,v) \mid u \in X,\ v \in Y \}$$



Definiere iterativ $X \times Y \times Z = (X \times Y) \times Z$ und überlege, dass die Klammern nicht wichtig sind

Ein Element u von $X_1 \times X_2 \times \dots \times X_n$ heißt

<u>n-Tupel</u> $u = (u_1, u_2, \dots, u_n)$ $\quad u_k \in X_k$

$k = 1, \dots, n$

(2-Tupel = Paar, 3-Tupel = Tripel)

#

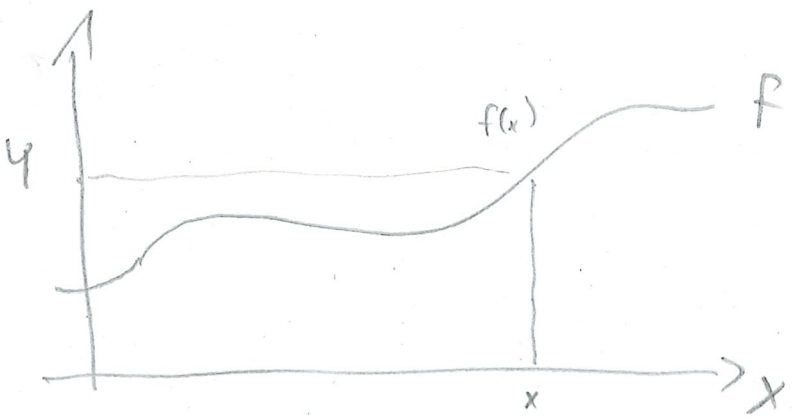
16. <u>Funktionen oder Abbildungen</u>

Seien X, Y Mengen, sei $F \subseteq X \times Y$ eine Menge von Paaren. Wir nennen f eine <u>Abbildung</u> oder <u>Funktion</u> von X nach Y, wenn es zu jedem $x \in X$ genau ein $y \in Y$ gibt mit $(x, y) \in F$.

Dann schreiben wir $f(x) = y$ sowie

$f: X \to Y$ oder $X \xrightarrow{f} Y$

oder $f: x \longmapsto f(x)$



Funktionen sind also Schaubilder oder Graphen.

Beispiel $X = Y = \mathbb{R}$

$$f = \{ (u,v) \in \mathbb{R} \times \mathbb{R} \mid v = u^2 \}.$$

Parabelfunktion

$f(x) = x^2$

Ist $A \subseteq X$ eine Teilmenge, so schreibt man kurz

$$f(A) = \{ f(a) \mid a \in A \} \subseteq Y,$$

das ist das Bild von A unter f.

Für $B \subseteq Y$ schreibt

$$f^{-1}(B) = \{ x \in X \mid f(x) \in B \} \subseteq X$$

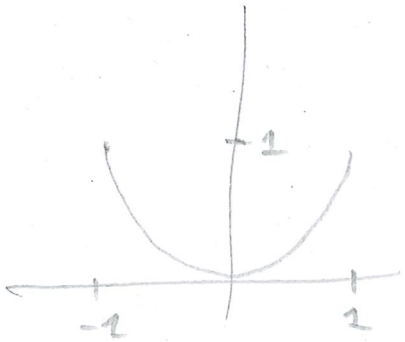
das ist das Urbild von B unter f.

Beispiel $f: \mathbb{R} \to \mathbb{R}$, $x \mapsto x^2$

Intervall $[a,b] = \{ t \in \mathbb{R} \mid a \leq t \leq b \}$

$f([0,1]) = [0,1]$

$f^{-1}([0,1]) = [-1,1]$



Es gilt immer

$f(f^{-1}(B)) \subseteq B$

$f^{-1}(f(A)) \supseteq A$

Für $P, Q \subseteq Y$ gilt

$f^{-1}(P \cap Q) = f^{-1}(P) \cap f^{-1}(Q)$

$f^{-1}(P \cup Q) = f^{-1}(P) \cup f^{-1}(Q)$

Eine Abbildung $f: X \to Y$ heißt

surjektiv, wenn $f(X) = Y$ gilt: zu jedem $y \in Y$ gibt es ein $x \in X$ mit $f(x) = y$

injektiv, wenn es zu jedem $y \in Y$ höchstens ein $x \in X$ gibt mit $f(x) = y$

bijektiv, wenn es zu jedem $y \in Y$ genau ein $x \in X$ gibt mit $f(x) = y$

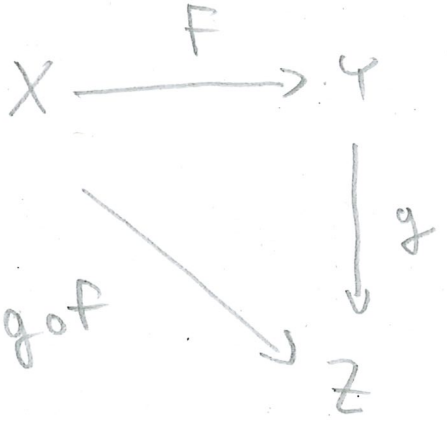
Bsp $h: \mathbb{Z} \to \mathbb{Z}$, $x \mapsto 2x$ ist
injektiv ($s \neq t \Rightarrow 2s \neq 2t$)
aber nicht surjektiv

$g: \mathbb{Z} \to \mathbb{N}$, $x \mapsto |x|$ ist surjektiv,
aber nicht injektiv ($g(2) = g(-2)$)

bijektiv = surjektiv + injektiv

Wenn $F: X \to Y$ und $g: Y \to Z$
Abbildungen sind, dann ist die Komposition
oder Verknüpfung oder Hintereinanderausführung $g \circ F: X \to Z$ die Abbildung

$$x \longmapsto g(f(x))$$



17. Relationen und Äquivalenzrelationen

Sei X eine Menge. Eine **zweistellige Relation** auf X ist eine Teilmenge $R \subseteq X \times X$,

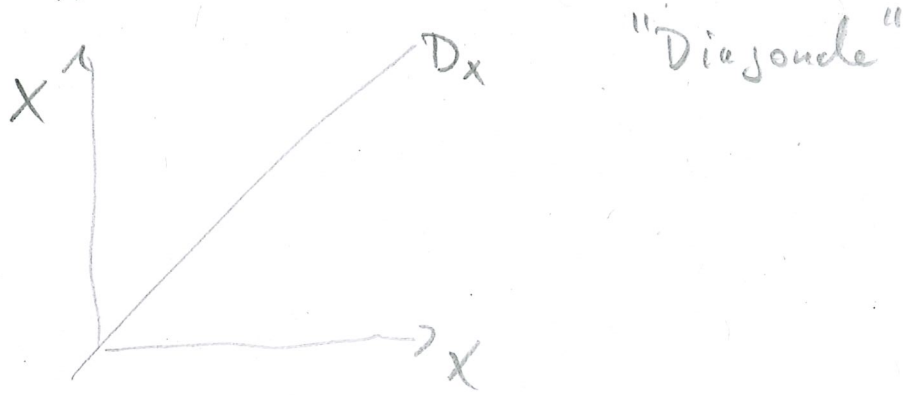
schreibe $uRv \iff (u,v) \in R$

$u \not R v \iff (u,v) \notin R$

Bsp (a) **Gleichheit**

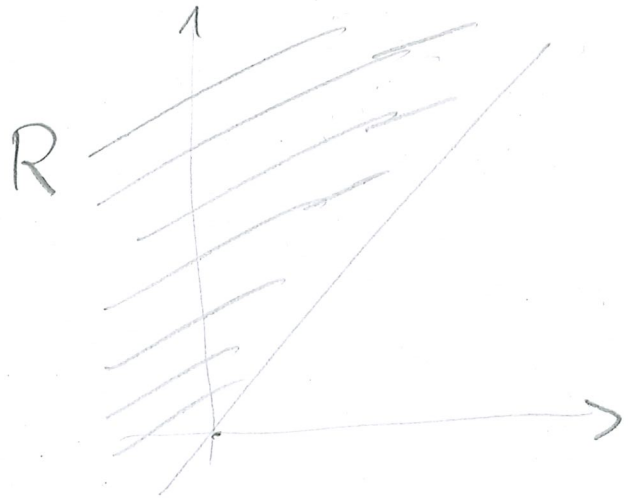
$$D_X = \{ (u,v) \in X \times X \mid u = v \}$$

"Diagonale"



(b) Anordnung $<$ auf $\mathbb{R}$

$$R = \{ (u,v) \in \mathbb{R} \times \mathbb{R} \mid u < v \}$$



18. Def Eine zweistellige Relation $R = \sim$ auf einer Menge X heißt **Äquivalenzrelation**, wenn folgendes gilt:

(ÄR1) $u \sim u$ gilt für alle $u \in X$ (Reflexivität)

(ÄR2) wenn $u \sim v$, dann gilt auch $v \sim u$ (Symmetrie)

(ÄR3) wenn $u \sim v$ und $v \sim w$, dann gilt auch $u \sim w$ (Transitivität)

Für $x \in X$ setzt $[x]_\sim = \{u \in X \mid u \sim x\} \subseteq X$ Äquivalenzklasse von x

sowie $X/\sim = \{[x]_\sim \mid x \in X\} \subseteq P(X)$

Beispiel (a) Gleichheit

$u \sim v \Leftrightarrow u = v$ ist ÄR

$[x)_= = \{x\}$

(b) alles $u \sim v$ für alle $u, v \in X$ ist ÄR

$[x]_\sim = X$

19. Die Zahlen als Mengen und Äquivalenzklassen

(a) Die natürlichen Zahlen lassen sich wie folgt als Mengen kodieren. Wir werden diese Kodierung aber im folgenden nie benutzen.

Definiere $s(a) = a \cup \{a\}$ wie im Zermelo-Fraenkel-Axiom (Inf) und setze nacheinander

$$0 = \phi$$
$$1 = s(0) = \phi \cup \{\phi\} = \{\phi\}$$
$$2 = s(1) = s(\{\phi\}) = \{\phi\} \cup \{\{\phi\}\} = \{\phi, \{\phi\}\}$$
$$3 = s(2) = \{\phi, \{\phi\}, \{\phi, \{\phi\}\}\}$$

usw

Das Axiom (Inf) garantiert die Existenz der Nachfolgerstruktur $(\mathbb{N}, \phi, s)$. → mathematische Logik

Die folgenden Konstruktionen sind wichtig für uns.

(b) Die ganzen Zahlen $\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$ konstruiert man aus $\mathbb{N}$ wie folgt. Betrachte auf $\mathbb{N}$ die Äquivalenzrelation

$$(x,y) \sim (u,v) \iff x+v = y+u$$

Idee (x,y) bedeutet die ganze Zahl $x-y$

(ÄR1) und (AR2) sind klar. Zu (AR3)

$$(x,y) \sim (u,v) \sim (p,q)$$

$$x+v = y+u \qquad u+q = p+v$$

also $\left.\begin{array}{l} u+q+y = p+v+y \\ \| \\ x+q+v \end{array}\right\} \Rightarrow x+q = p+y$

d.h. $(x,y) \sim (p,q)$

Nun kann man Addition und Multiplikation auf $\mathbb{Z}$ definieren, etwa

$$[(x,y)]_\sim + [(u,v)]_\sim = [(x+u, y+v)]_\sim$$

$$[(x,y)]_\sim \cdot [(u,v)]_\sim = [(xu+yv, yu+xv)]_\sim$$

(c) Die rationalen Zahlen $\mathbb{Q} = \{ \frac{a}{b} \mid a,b \in \mathbb{Z}, b \neq 0 \}$

Äquivalenzrelation $\sim$ auf $\mathbb{Z}$ durch

$(a,b) \sim (p,q)$ $\quad b,q \neq 0$

$\Leftrightarrow \quad a \cdot q = b \cdot p$ (die (a,b) kodiert den Bruch $\frac{a}{b}$.