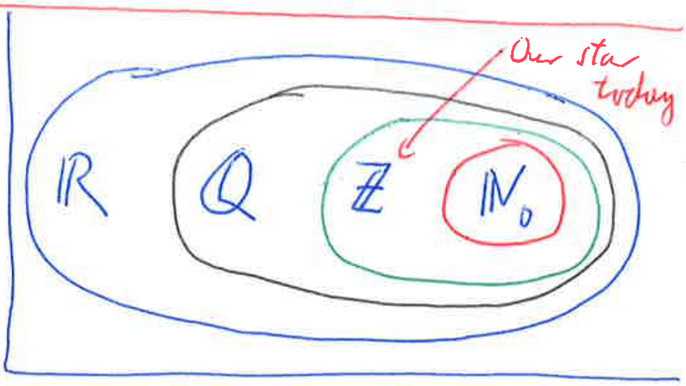
Vorlesung 9, 15. Nov. 2018

"Die rationalen Zahlen I"



Sei $\otimes : X \times X \to X$ eine Verknüpfung mit Einheit e. Dann heißt $x \in X$ <u>invertierbar</u> (bzgl. $\otimes$) mit <u>Inverse</u> x^{-1} falls $x^{-1} \in X$ existiert und $x \otimes x^{-1} = e = x^{-1} \otimes x$ gilt.

Wie immer sind Inverse eindeutig, falls existent:

$$x^{-1} = x^{-1} \otimes x \otimes \tilde{x}^{-1} = \tilde{x}^{-1}$$

<u>Beispiel 9.1</u> $\mathbb{N}_0$ hat zwei Verknüpfungen, $+$ und $\cdot$, mit Einheiten 0 und 1. Aber kein Element $n \in \mathbb{N}_0$ $(n \neq 1)$ ist invertierbar, weder bzgl. $+$ noch $\cdot$, denn

$$m + n = 0 \Rightarrow m = n = 0 \quad \text{bzw.} \quad m \cdot n = 1 \Rightarrow m = n = 1$$

Genau das wollen wir "beheben" und führen dazu $\mathbb{Z}$ (heute) bzw. $\mathbb{Q}$ ein (nächstes Mal)

<u>Konvention 9.2:</u> Im Folgenden bezeichnet $+$ eine assoziative und kommutative Verknüpfung mit Einheit 0 ← genannt <u>Null</u>, und $\cdot$ eine assoziative und kommutative Verknüpfung mit Einheit 1. ← genannt <u>Eins</u>

$\boxed{\text{Vorsicht: Diese müssen nicht auf } \mathbb{N}_0 \text{ sein,}}$

Außerdem, falls $+, \cdot$ auf einer Menge sind, bindet $\cdot$ stärker, d.h. $a \cdot b + c = (a \cdot b) + c$ etc.

Ein kommutativer Ring R mit Eins, kurz: Ring, ist eine Menge R mit $\boxed{\text{zwei Verknüpfungen}}$

$+ : R \times R \longrightarrow R \qquad \cdot : R \times R \longrightarrow R$

welche $\boxed{\text{distributiv}}$ sind

$$(a+b)c = ac + bc \quad \forall\, a,b,c \in R$$

und jedes Element $a \in R$ ist $\boxed{\text{bzgl. + invertierbar}}$

Vorsicht: Im allgemeinen fordert man nicht, dass $\cdot$ kommutativ ist und eine Einheit besitzt.

Das Inverse von a wird mit $-a$ bezeichnet, also $a + (-a) = a - a = 0 = (-a) + a$

Für folgende Tatsache sei auf [AE06, Bemerkungen 8.1] verwiesen:

- Für alle $a,b \in R$ hat $a + x = b$ eine Lösung, nämlich $x = b + (-a) = b - a$, genannt Differenz. (Man kann + kürzen)
- Für $\forall\, a \in R$ gilt $a0 = 0a = 0$
- Es kann $a,b \neq 0$ geben mit $ab = 0$. Deswegen besitzt $ab = x$ im Allgemeinen keine Lösung. (Man kann $\cdot$ nicht kürzen.)
- Es gilt $a(-b) = (-a)b = -(ab) = -ab$ und $(-a)(-b) = ab$
- Es gilt $(-1)a = -a$.
- Rekursiv kann man $n \cdot a = \text{“}na\text{”}$ $\overbrace{}^{a+\dots+a}$ und $a^n = a\cdots a$ definieren. Analog für endl. Produkte und Summen

---

Beispiel 9.3 Ist R ein Ring, so ist $R \times R$ auch ein Ring, wobei die Multiplikation und Addition

Komponentenweise definiert sind: ↷ Null ist $(0,0)$

$$(a_1,a_2)+(b_1,b_2)=(a_1+b_1,\ a_2+b_2)$$

$$(a_1,a_2)\cdot(b_1,b_2)=(a_1b_1,\ a_2b_2)$$ Eins ist $(1,1)$

Damit gilt insbesondere $(1,0)\cdot(0,1)=(1\cdot 0,\ 0\cdot 1)=(0,0)$

Analog für alle endliche Produkte.

Beispiel 9.4 Für unendliche Produkte R^X kann man durch

$$(f+g)(x)=f(x)+g(x) \qquad x\in X$$

$$(fg)(x)=f(x)\,g(x) \qquad f,g\in R^X=\mathrm{Abb}(X,R)$$

eine Ringstruktur definieren. Null ist die Abbildung $f(x)=0$, Eins die Abbildung $f(x)=1$.

Theorem 9.5 (Binomische Satz)

Sei R ein Ring. Dann gilt $\forall a,b\in R\ \ \forall n\in\mathbb{N}_0$:

$$(*) \quad (a+b)^n=\sum_{k=0}^{n}\binom{n}{k}a^kb^{n-k},$$

wobei $\binom{n}{k}=\begin{cases}\frac{n!}{k!(n-k)!} & \leftarrow \in\mathbb{N}_0 \text{ wegen Übungsaufgabe 7.1}\\ 0, & \text{falls } k>n\end{cases}$ $\quad n,k\in\mathbb{N}_0$

Beweis: Bemerke zuerst, dass beide Seiten von $(*)$ wohldefiniert sind.

Weiter: Behauptung: Es gilt $\binom{n}{k-1}+\binom{n}{k}=\binom{n+1}{k}$ für $1\le k\le n$.

Beweis: Ausgelassen. (Induktion nach n)

Nun ~~[illegible]~~ Induktion nach n.

(IA): $n=0$ ist wahr, denn $(a+b)^0 = 1 = \sum_{k=0}^{0} \binom{0}{k} a^k b^{n-k}$.

(IS): Gelte (*) nun also für n.

Dann $(a+b)^{n+1} = (a+b)^n (a+b)$

$$\overset{\text{Induktion}}{=} \left(\sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} \right)(a+b)$$

$$= \sum_{k=0}^{n} \binom{n}{k} a^{k+1} b^{n-k} + \sum_{k=0}^{n} \binom{n}{k} a^k b^{n+1-k}$$

$$= a^{n+1} + \left(\sum_{k=0}^{n-1} \binom{n}{k} a^{k+1} b^{n-k} \right) + \left(\sum_{k=1}^{n} \binom{n}{k} a^k b^{n+1-k} \right) + b^{n+1}$$

$$= a^{n+1} + \left(\sum_{k=1}^{n} \left[\binom{n}{k-1} + \binom{n}{k} \right] a^k b^{n+1-k} \right) + b^{n+1}$$

$$= a^{n+1} + \sum_{k=1}^{n} \binom{n+1}{k} a^k b^{n+1-k} + b^{n+1} \quad \Box$$

<u>Beispiel 9.6</u> Es gilt $(a+b)^0 = 1$,
$(a+b)^2 = a^2 + 2ab + b^2$, $(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$
etc. und das gilt in jedem Ring.

Zurück zu $\mathbb{N}_0$: Dies ist beinahe ein Ring, es fehlen die Inversen, also "$-n$".

Idee: Nehmen wir an Z sei ein Ring mit $Z \supset \mathbb{N}_0$ so, dass $+, \cdot$ von Z mit den von $\mathbb{N}_0$ übereinstimmt.

Dann ist aber $m - n \in Z$ für $(m,n) \in \mathbb{N}_0^2$

definiert. Abgesehen:

$$\underbrace{m-n = m'-n'}_{\text{in } \mathbb{Z}} \iff \underbrace{m+n' = m'+n}_{\text{in } \mathbb{N}_0}$$

Diese Betrachtung legt nahe $\mathbb{Z}$ aus Zahlenpaaren $(m,n) \in \mathbb{N}_0^2$ zu konstruieren. In der Tat:

Theorem 9.7 Es gibt einen kleinsten, nullteilerfreien Ring $\boxed{\mathbb{Z}} \supset \mathbb{N}_0$, der auf $\mathbb{N}_0$ die ursprüngliche $+$ und $\cdot$ induziert. Dieser Ring ist bis auf Isomorphie eindeutig und wird Ring der ganzen Zahlen genannt.

Bemerkung 9.8 – "kleinste" bedeutet, dass jeder andere Ring R mit diesen Eigenschaften $R \supset \mathbb{Z}$ erfüllt (mit induzierten $+, \cdot$)

– "nullteilerfrei" heißt $a \cdot b = 0 \iff (a=0 \vee b=0)$

– "Ein Isomorphismus von Ringen $(R,+,\cdot)$ und $(Q,\tilde{+},\tilde{\cdot})$ ist eine Bijektion $\varphi: R \longrightarrow Q$ so, dass "die Ringstruktur erhalten wird", d.h.

$$\varphi(a+b) = \varphi(a) \tilde{+} \varphi(b), \quad \varphi(a \cdot b) = \varphi(a) \tilde{\cdot} \varphi(b)$$

$$\varphi(0_R) = 0_Q \quad ; \quad \varphi(1_R) = 1_Q$$

Das ist der technische Ausdruck für "als Ringe gleich bis auf Umbenennung" (Details [AE06, Sektion I.8].).

Beweis (Skizze, denn der echte Beweis ist lang)

Schritt 1: Definiere auf $\mathbb{N}_0 \times \mathbb{N}_0$ eine Relation $\sim$ durch

$$(m,n) \sim (m',n') \iff m+n' = m'+n.$$

Dies ist eine Äquivalenzrelation, denn

Reflexiv $(m,n) \sim (m,n)$, da $m+n = m+n$

Symmetrisch $(m,n) \sim (m',n')$, da $m+n = n+m$
$\Rightarrow (m',n') \sim (m,n)$

$m+n' = m'+n$ $\qquad$ $m'+n'' = m''+n'$

Transitiv $(m,n) \sim (m',n') \wedge (m',n') \sim (m'',n'')$, wegen Kürzungsregel
$\Rightarrow (m,n) \sim (m'',n'') \to m+n'' = m''+n$

$m+n'+n'' = m'+n+n''$

$m+n''+n'$ $\qquad$ $m''+n+n'$

Schritt 2:

Setze $\mathbb{Z} = \mathbb{N}_0^2/\sim$ und notiere $\underset{[(n,0)]}{\overset{\shortparallel}{n}} \in \mathbb{Z}$, $\underset{[(0,n)]}{\overset{\shortparallel}{-n}} \in \mathbb{Z}$ für $n \in \mathbb{N}_0$

Definiere:

$$[(m,n)] + [(m',n')] = [(m+m', n+n')]$$
$$[(m,n)] \cdot [(m',n')] = [(mm'+nn', mn'+n'n)]$$

Dann ist $[(0,0)] + [(m,n)] = [(m,n)]$
und $+_{\mathbb{Z}}$ ist kommutativ und assoziativ,
da $+_{\mathbb{N}_0}$ beides ist. $\quad$ Null in $\mathbb{Z}$

Man überlege sich, warum das wohldefiniert ist...

Analog, man sieht durch ausrechnen,
dass $\cdot_{\mathbb{Z}}$ kommutativ und assoziativ

ist, da $+_{\mathbb{N}_0}, \circ_{\mathbb{N}_0}$ dies sind und ~~be~~ zusammen distributiv sind. Auch ist

$$\underbrace{[(1,0)]}_{\text{Eins in } \mathbb{Z}} \cdot [(m,n)] = [(m,n)]$$

Schritt 3:

Und weiter gibt es einen ~~Ringisomorphismus~~ Abbildung: $\varphi : \mathbb{N}_0 \longrightarrow \mathbb{Z}$

$$n \longmapsto [(n,0)] = n$$

welche injektiv ist und $\varphi(0) = 0_{\mathbb{Z}}$, $\varphi(1) = 1_{\mathbb{Z}}$

$\varphi(m+n) = \varphi(m) +_{\mathbb{Z}} \varphi(n)$ und $\varphi(mn) = \varphi(m) \cdot_{\mathbb{Z}} \varphi(n)$

Schritt 4: Es gilt $n + (-n) = 0$, denn

$$[(n,0)] + [(0,n)] = [(n,n)], \text{ aber}$$

$$(n,n) \sim (0,0), \text{ denn } n + 0 = \cancel{n+0}\ 0 + n$$

Also gibt es Inverse.

Zusammen: Schritte 1–4 zeigen, dass $\mathbb{Z}$ ein Ring ist, welcher $\mathbb{N}_0$ enthält.

Schritt 5: $\underbrace{[(m,n)]}_{a} \cdot \underbrace{[(m',n')]}_{b} = [(mm'+nn'),(mn'+m'n)] = 0_{\mathbb{Z}}$

$\iff m = n$ oder $m' = n'$ $\iff a = 0 \lor b = 0$

Schritt 6: $\mathbb{Z}$ ist minimal, da exakt die $+$-Inversen hinzugefügt werden "$\mathbb{Z} = -\mathbb{N}_{\cancel{0}} \cup \underbrace{\{0\} \cup \mathbb{N}}_{\mathbb{N}_0}$"

Schritt 7: Man baut induktiv einen Ringisomorphismus zu anderen minimalen Konstruktionen.