Rückblick auf die bisherigen Kapitel

§ 1. Aussagenlogik, logische Verknüpfungen ($\neg$, $\wedge$, $\vee$, $\Rightarrow$, $\Leftrightarrow$)

§ 2. Einführung des Mengenbegriffs, Mengenoperationen ($\cap$, $\cup$, $\setminus$, $\times$, $\mathscr{P}$), Prädikatenlogik ($\forall\, x \in A : P(x)$, $\exists\, x \in A : P(x)$), Prinzip der vollständigen Induktion

§ 3. Relationsbegriff, Halb- und Totalordnungen, Äquivalenzrelationen (Beispiel: $\equiv_n$)

§ 4. erster Teil:
Abbildungen, Bild- und Urbildmengen, Eigenschaften von Abbildungen (injektiv, surjektiv und bijektiv)

§ 4. zweiter Teil:
Definition der Mächtigkeit $|A| \in \mathbb{N}_0$ einer endlichen Menge, Rechenregeln für Mächtigkeiten, Binomialkoeffizienten, unendliche Mengen: Unterscheidung von abzählbar unendlichen Mengen ($\mathbb{N}$, $\mathbb{N}_0$, $\mathbb{Z}$, $\mathbb{Q}$) und überabzählbaren Mengen ($\mathbb{R}$, $\mathbb{C}$)

Definition (5.1)

Eine Verknüpfung auf einer Menge A ist eine Abbildung $A \times A \to A$.

- Beispiele für Verknüpfungen auf $\mathbb{R}$ sind die Addition, die Subtraktion oder die Multiplikation.
- Man unterscheidet bei Verknüpfungen zwischen multiplikativer und additiver Schreibweise. Additive („plusartige“) Verknüpfungssymbole sind $+$, $\oplus$ oder $\boxplus$. Multiplikative Verknüpfungssymbole sind $\cdot$, $\odot$ oder $*$.

Eigenschaften von Verknüpfungen

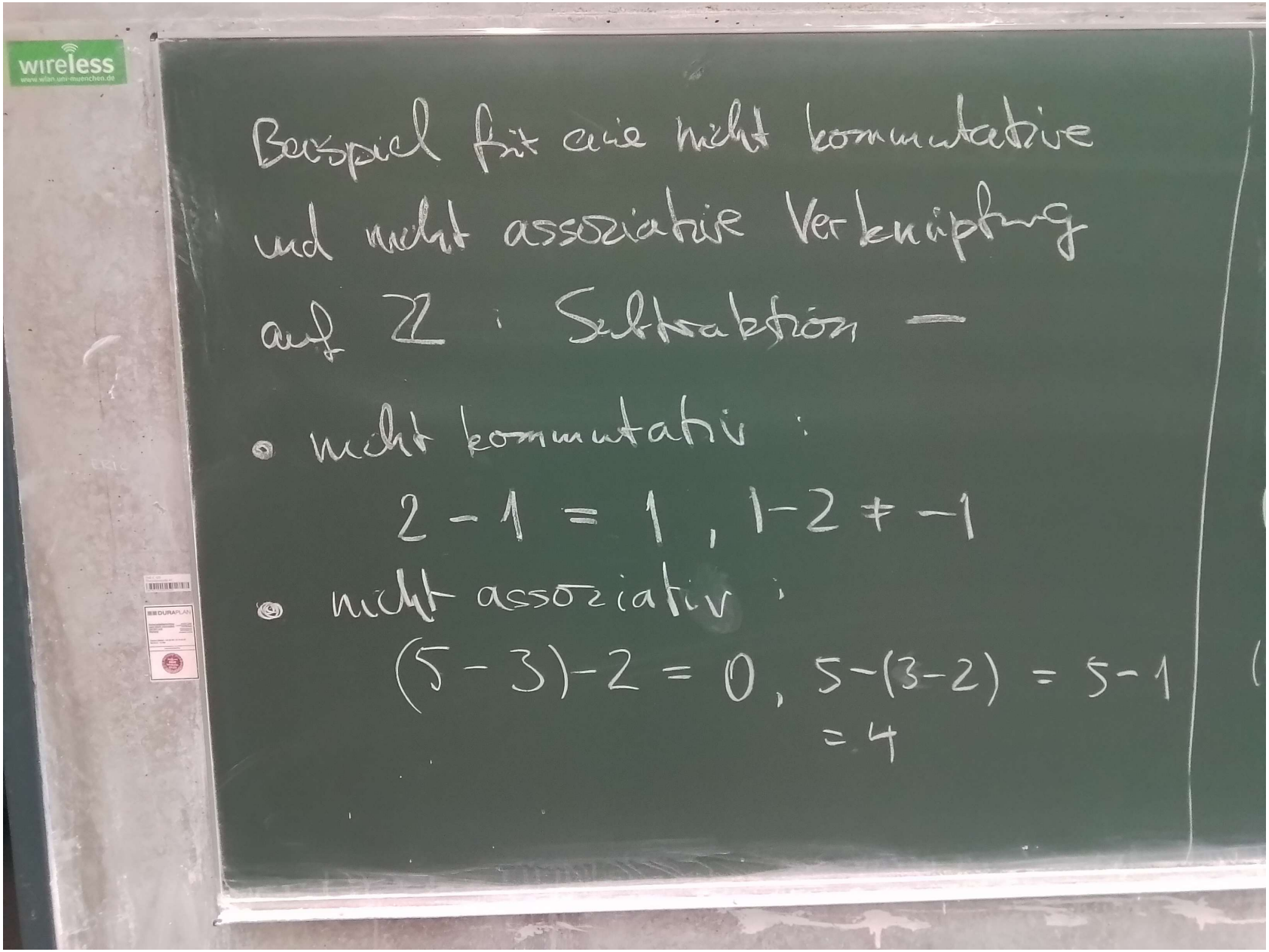
Definition (5.2)

Eine Verknüpfung $\cdot$ auf einer Menge A bezeichnet man als

(i) kommutativ, wenn $ab = ba$ für alle $a, b \in A$

(ii) assoziativ, wenn $a(bc) = (ab)c$ für alle $a, b, c \in A$ erfüllt ist.

Man bezeichnet eine Teilmenge $B \subseteq A$ als abgeschlossen unter der Verknüpfung $\cdot$, wenn für alle $b, b' \in B$ jeweils $bb' \in B$ gilt. Man erhält in diesem Fall eine Verknüpfung $\cdot_B$ auf B, indem man $b \cdot_B b' = bb'$ für alle $b, b' \in B$ setzt.



Korrektur 5. Zeile: $2 - 1 = 1$, $1 - 2 = -1$, $1 \neq -1$

Beispiele für abgeschlossene Teilmengen bezüglich einer Verknüpfung

(1) $\mathbb{N}$ sind abgeschlossen bezüglich der Addition und der Multiplikation auf $\mathbb{R}$

(2) $\mathbb{Z}$ ist abgeschlossen bzgl. der Subtraktion auf $\mathbb{R}$

(3) $\mathbb{N}$ ist <u>nicht</u> abgeschl bzgl. der Subtraktion auf $\mathbb{R}$
(Bsp.: $2, 3 \in \mathbb{N}$, aber $2-3 \notin \mathbb{N}$)

(4) $\{0\}$ ist in $\mathbb{R}$ abgeschl. bzgl. $+$ und $\cdot$
$\{1\}$ ist in $\mathbb{R}$ abgeschl. bzgl. $\cdot$, aber nicht bzgl. $+$

Definition (5.3)

(i) Eine Halbgruppe ist ein Paar $(G, \cdot)$ bestehend aus einer nichtleeren Menge G und einer assoziativen Verknüpfung $\cdot$ auf der Menge G.

(ii) Ein Element $e \in G$ in einer Halbgruppe wird Neutralelement genannt, wenn $g \cdot e = e \cdot g = g$ für alle $g \in G$ erfüllt ist.

(iii) Eine Halbgruppe $(G, \cdot)$, in der ein Neutralelement existiert, wird Monoid genannt.

Beispiele für Halbgruppen und Monoide:

(1) $(\mathbb{N}, +)$, $(\mathbb{N}_0, +)$, $(\mathbb{Z}, +)$
$(\mathbb{N}, \cdot)$, $(\mathbb{N}_0, \cdot)$, $(\mathbb{Z}, \cdot)$
sind Halbgruppen

(2) $(\mathbb{N}_0, +)$ ist Monoid (0 Neutralelement)
$(\mathbb{Z}, +)$ " " (0 ")
$(\mathbb{N}, \cdot)$ ist Monoid (1 Neutralelement)
$(\mathbb{N}_0, \cdot)$ " " " "
$(\mathbb{Z}, \cdot)$ " " " "

Invertierbar Elemente

Definition (5.4)

(i) Ein Element g in einem Monoid $(G, \cdot)$ mit Neutralelement e heißt invertierbar, wenn ein $h \in G$ existierst, so dass die Gleichungen $g \cdot h = h \cdot g = e$ erfüllt sind.

(ii) Eine Gruppe ist ein Monoid, in dem jedes Element invertierbar ist.

(iii) Eine Halbgruppe, und ebenso ein Monoid und eine Gruppe, wird kommutativ oder abelsch genannt, wenn die zugehörige Verknüpfung kommutativ ist.

Beispiele für invertierbare Elemente:

(1) $(\mathbb{N}_0, +)$ a invertierbar $\Leftrightarrow \exists\, b \in \mathbb{N}_0 : a+b = b+a = 0$ ist einziges invertierbares Element

(2) $(\mathbb{Z}, +)$ Jedes $a \in \mathbb{Z}$ ist invertierbar, denn es gilt $a + (-a) = (-a) + a = 0$. Z.B ist -2 das Inverse von 2 im Monoid $(\mathbb{Z}, +)$.
($\Rightarrow (\mathbb{Z}, +)$ ist eine Gruppe)

(3) $(\mathbb{N}, \cdot)$: einziges invertierbares Element: 1

(4) $(\mathbb{N}_0, \cdot)$: " " " : 1

(5) $(\mathbb{Z}, \cdot)$: einzige invertierbare Elemente: ± 1

Rechenregeln in Monoiden

Lemma (5.5)

Sei $(G, \cdot)$ ein Monoid, und sei e ein Neutralelement des Monoids.

(i) Das Monoid besitzt keine weiteren Neutralelemente. Man bezeichnet e deshalb als *das* Neutralelement des Monoids, und bezeichnet es mit e_G.

(ii) Zu jedem invertierbaren Element $a \in G$ gibt es genau ein Element $b \in G$ mit $ab = ba = e_G$. Man nennt b das zu a inverse Element, und bezeichnet es mit a^{-1}.

(iii) Ist a invertierbar und $b \in G$ ein Element mit $ab = e_G$, dann folgt daraus bereits $b = a^{-1}$. Ebenso folgt bereits aus der Gleichung $ba = e_G$, dass b das Inverse von a ist.

(iv) Das Neutralelement ist invertierbar, und es gilt $e_G^{-1} = e_G$.

(v) Sind a und b invertierbare Elemente des Monoids, dann sind auch ab und a^{-1} invertierbar, und es gilt $(ab)^{-1} = b^{-1}a^{-1}$ und $(a^{-1})^{-1} = a$.

Beweis von Lemma 5.5

zu (i) Ang., e und e' sind beides Neutralelemente $\Rightarrow \forall a \in G$:

$$a \circ e = a \,, \quad e \cdot a \overset{(*_2)}{=} a$$

$$a \cdot e' \overset{(*_1)}{=} a \,, \quad e' \cdot a = a$$

$$\Rightarrow e \overset{(*_1)}{=} e \cdot e' \overset{(*_2)}{=} e'$$

angew. auf e angew. auf e'

zu (ii) Ang., es gibt ein $a \in G$, so dass b und c beides Inverse von a sind.

$$b = b \cdot e = b \cdot (a \cdot c) = (b \cdot a) \cdot c =$$

$$e \cdot c = c$$

(iii) Sei $a \in G$ invertierbar und $b \in G$ mit $a \cdot b = e_G$.

$\Rightarrow b = e \cdot b = (a^{-1} \cdot a) \cdot b = a^{-1} \cdot (a \cdot b)$

$= a^{-1} \cdot e = a^{-1}$ Der Beweis der zweiten Regel läuft analog.

(iv) Ein Element $c \in G$ ist genau dann Inverses von e, wenn $c \cdot e = e$ und $e \cdot c = e$. Diese Gleichungen werden von $c = e$ erfüllt. Also ist e sein eigenes Inverses, d.h. $e^{-1} = e$.

(v) Seien $a, b \in G$ invertierbare Elemente.

Rechne nach, dass $b^{-1}a^{-1}$ die Eigenschaften des Inversen von $a \cdot b$ besitzt. $(b^{-1} \cdot a^{-1}) \cdot (a \cdot b) = b^{-1} \cdot (a^{-1} \cdot a) \cdot b$

$= b^{-1} \cdot e \cdot b = b^{-1} \cdot b = e$

$(a \cdot b) \cdot (b^{-1} \cdot a^{-1}) = a \cdot (b \cdot b^{-1}) \cdot a^{-1}$

$= a \cdot e \cdot a^{-1} = a \cdot a^{-1} = e$

Beh. a ist Inverses von a^{-1}, d.h. $a = (a^{-1})^{-1}$

Überprüfe: a erfüllt die Bedingungen für das Inverse von a^{-1}. Tatsächlich gilt $a \cdot a^{-1} = e$, $a^{-1} \cdot a = e$.

$\Rightarrow a$ ist das Inverse von a^{-1}.

Die Gruppe der invertierbaren Elemente

Folgerung (5.6)

Sei $(G, \cdot)$ ein Monoid, und sei $G^\times \subseteq G$ die Teilmenge der invertierbaren Elemente. Dann ist $G^\times$ bezüglich $\cdot$ abgeschlossen, und $(G^\times, \cdot_{G^\times})$ ist eine Gruppe.

Bem.: Sei $(A, +)$ ein Monoid (mit einem additiven Verknüpfungssymbol).

- Das Neutralelement wird dann üblicherweise nicht mit e, sondern mit 0 (oder 0_A) bezeichnet.
- Das Inverse eines invertierbaren Elements wird nicht mit a^{-1}, sondern mit $-a$ bezeichnet.

Definition der Ringe

Definition (5.7)

Ein Ring ist ein Tripel $(R, +, \cdot)$ bestehend aus einer Menge R und zwei Verknüpfungen $+$ und $\cdot$ auf R mit folgenden Eigenschaften.

(i) Das Paar $(R, +)$ ist eine abelsche Gruppe.

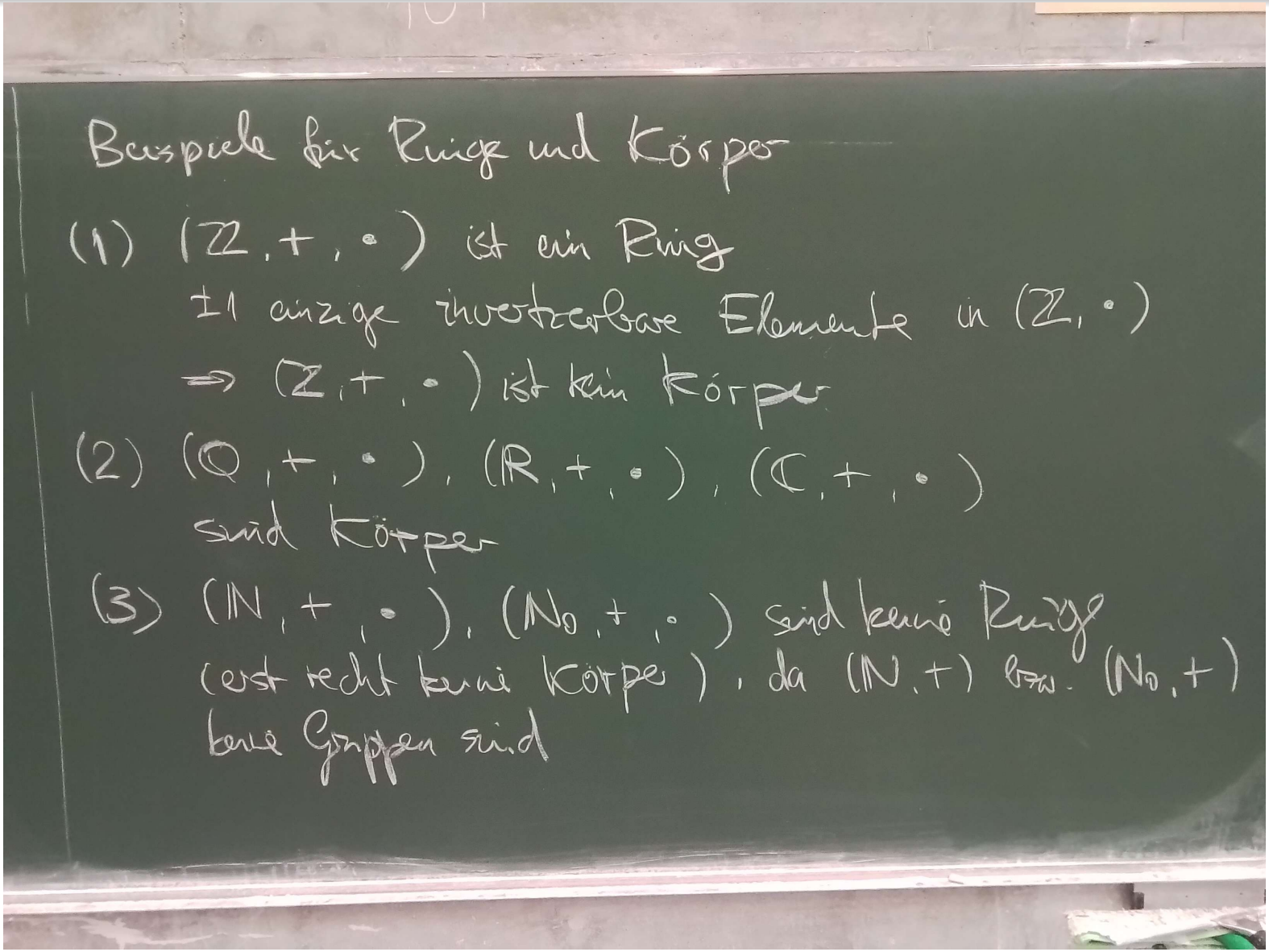
(ii) Das Paar $(R, \cdot)$ ist ein abelsches Monoid.

(iii) Es gilt das Distributivgesetz $a(b + c) = ab + ac$ für alle $a, b, c \in R$.

Ergänzungen zur Ringdefinition

Sei $(R, +, \cdot)$ ein Ring.

- Das Neutralelement der Gruppe $(R, +)$ wird das Nullelement des Rings genannt und mit 0_R bezeichnet.
- Für jedes $a \in R$ nennt man das inverse Element von a in $(R, +)$ das Negative von a und bezeichnet es mit $-a$.
- Die Subtraktion auf R definiert man durch $a - b = a + (-b)$ für alle $a, b \in R$.
- Das Neutralelement des Monoids $(R, \cdot)$ nennt man das Einselement des Rings und bezeichnet es mit 1_R.
- Wenn die Menge $R^\times$ der invertierbaren Elemente des Monoids $(R, \cdot)$ mit $R \setminus \{0_R\}$ übereinstimmt, dann bezeichnet man den Ring auch als Körper.



(In der 4. Zeile stand erst $(\mathbb{Z}, +, , \cdot)$ ist ein Körper, das war ein Schreibfehler. Weil nicht jedes Element aus $\mathbb{Z} \setminus \{0\}$ bezüglich $\cdot$ invertierbar ist, ist die Struktur definitiv kein Körper.)