1 Gruppen, Ringe, Körper

1.1 Ringe

Definition 1 (Ring)**.** Ein Ring $R = (R, +, \cdot, O_R)$ ist eine Menge R und zwei Verknüpfungen $+, \cdot : R \times R \to R$ und einem Element $O_R \in R$ so dass:

1. $(R, +, O_R)$ ist eine abelsche Gruppe
2. $a \cdot (b \cdot c) = (a \cdot b) \cdot c \ \forall a, b, c \in R$
3. $a \cdot (b + c) = a \cdot b + a \cdot c$, $(a + b) \cdot c = ac + bc$

Ein unitärer Ring („Ring mit 1") ist ein Tupel $(R, +, \cdot, 0_R, 1_R)$, so dass $(R, +, \cdot, 0_R)$ ein Ring ist und $1_R \in R$, so dass gilt:

1. $1_R \cdot a = a = a \cdot 1_R$

Ein Ring heißt kommutativ, wenn

1. $a \cdot b = b \cdot a \ \forall a, b \in R$

Bemerkung 1 (Notation)**.** Das inverse Element von $a \in R$ bezüglich $+$ bezeichnet man mit $-a$. Ein Inverses bezüglich $\cdot$ existiert i.A. nicht.

Die Eins in einem unitären Ring ist eindeutig bestimmt.

Beispiel 1. $(\mathbb{Z}, +, \cdot, 0, 1)$ ist ein kommutativer Ring mit 1

Beispiel 2 $(\mathbb{Z}/n\mathbb{Z})$**.** ist ein kommutativer Ring mit 1. Multiplikationsvorschrift ist die folgende: Für $A, B \in \mathbb{Z}/n\mathbb{Z}$

1. Wähle Vertreter $a, b \in \mathbb{Z}$ von A und B.
2. bilde $a \cdot b$ in $\mathbb{Z}$
3. $A \cdot B :=$ Restklasse von $a \cdot b$

Nachzuweisen: Unabhängigkeit der Definition von der Auswahl der Vertreter im ersten Schritt.

Beispiel 3 (Die Menge der geraden ganzen Zahlen)**.** ist ein kommutativer Ring ohne 1.

Lemma 1. $R = (R, +, \cdot, 0_R)$ Ring. Dann gilt

1. $0_R \cdot a = 0_R = a \cdot 0_R$
2. $a \cdot (-b) = -ab = (-a) \cdot b$

Ist R unitär, so gilt:

1. $-b = (-1_R) \cdot b$

Beweis 1.

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

Mit kürzen folgt: $0_R = 0_R a$ Analog für $a \cdot 0_R = 0_R$ □

Beweis 2.

$$0_R = a0_R = a\left((-b) + b\right) = a(-b) + ab$$

also $a(-b) = -ab$. □

Beweis 3. Ist R unitär, so setzt man in 2 $a = 1_R$ ein und erhält 3. □

Beispiel 4. $R = \{0\}$ mit den einzig möglichen Verknüpfungen + und · heißt der *Nullring*. Nullring ist ein kommutativer Ring mit 1 ($0_R = 0 = 1_R$). Dies ist der einzige Ring mit $1_R = 0_R$.

Begründung: Gelte $0_R = 1_R$, so folgt für jedes $r \in R$:

$$r = r \cdot 1_R = r \cdot 0_R = 0_R.$$

Egal welches Element herausgenommen wird, es ist immer 0_R, d.h. R muss ein Nullring sein.

Lemma 2. Sei $R = (R, +, \cdot, 0_R, 1_R)$ ein unitärer Ring und $R^\times \subset R$ die Menge der Elemente die ein Links- und ein Rechtsinverses bezüglich · haben, das heißt

$$R^\times = \{r \in R \mid \exists s, t \in R : sr = 1_R = rt\}.$$

Dann ist $(R^x, \cdot, 1_R)$ eine Gruppe. Man nennt R^x die Einheitengruppe von R.

Beweis. Seien $r, \overline{r} \in R^\times$ und $s, \overline{s}, t, \overline{t}$ mit

$$sr = 1 = rt.$$

und

$$\overline{sr} = 1 = \overline{r}\overline{t}.$$

Dann

$$(s's)(rr') = s'(sr)r' = s'1r' = s'r' = 1.$$
$$(rr')(t't) = r(r't')t = r1t = rt = 1.$$

$\implies r \cdot r' \in R^\times$

Wir überprüfen die Gruppenaxiome: G1 folgt aus R2

$1 \in R$ ist neutral → G2

Bleibt zu zeigen: $\forall r \in R^\times : \exists r' \in R : rr' = 1$ Nach Definition: $\exists s \in R : sr = 1$. Zu zeigen: $s \in R^\times$. Offenbar hat das Rechtsinverse r. Aber r ist auch linksinvers zu s:

Wähle $t \in R$ mit $rt = 1$. Dann gilt $s = s(rt) = (sr)t = t \implies$ rs = rt = 1. □

Bemerkung 2. $0_R \in R^\times \implies \exists r \in R : 0_R r = 1_R \implies 0_R = 1_R \implies R$ ist der Nullring.

Definition 2 (Körper)**.** Ein Körper K ist ein kommutativer Ring mit 1: $(K, +, 0_K, 1_K)$ mit $K^\times = K \setminus \{0_K\}$

Beispiel 5.
1. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sind Körper
2. $\mathbb{Z}$ ist kein Körper ($\mathbb{Z}^\times = \{+1, -1\}$)

Lemma 3. In einem Körper K gilt, dass

$$ab = 0_K \implies a = 0 \wedge b = 0.$$

Beweis. Angenommen $a \neq 0_K$: Dann existiert $a^{-1} \in K$ mit $a^{-1}a = 1_K$. Es folgt

$$b = 1_K b = a^{-1}ab = a^{-1}0_K = 0_K.$$

□

Lemma 4. Ist p eine Primzahl, so ist $\mathbb{Z}/p\mathbb{Z}$ ein Körper.

. $\mathbb{Z}/p\mathbb{Z}$ ist kommutativer Ring mit 1 (siehe oben).

Zu zeigen: $\forall A \in \mathbb{Z}/p\mathbb{Z}, A \neq \overline{0}$ ist die $\overline{1}$ im Bild der Abbildung:

$$A\cdot : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}, B \mapsto A \cdot B.$$

Wir zeigen sogar, dass $A\cdot$ surjektiv ist. Da $\mathbb{Z}/p\mathbb{Z}$ endlich ist, genügt es z.z., dass $A\cdot$ injektiv ist.

Angenommen es gäbe Restklassen $B, C \in \mathbb{Z}/p\mathbb{Z}$ mit

$$A \cdot B = A \cdot C.$$

Seien $a, b, c \in \mathbb{Z}$ Vertreter. Wegen $A \neq \overline{0}$ gilt a nicht durch p teilbar. Wegen $AB = AC$ gilt $ab = -ac \mod p \implies p$ teilt $a(b-c)$.

Weil p eine Primzahl ist und p teilt nicht a folgt $p/(b-c)$, also $b = -c \mod p \implies B = C$ □

Bemerkung 3. Ist $n \in N$ keine Primzahl, so ist $\mathbb{Z}/n\mathbb{Z}$ kein Körper.

Beweis. Für $n = 1$ ist $\mathbb{Z}/n\mathbb{Z}$ der Nullring (kein Körper).

Nun sei $n > 1$ keine Primzahl $\implies \exists a, b \in \mathbb{N}, 1 < a, b < n$ mit $ab = n$ Für die Restklassen bedeutet dies: $\overline{a} \neq \overline{0}$, $\overline{b} \neq \overline{0}$ aber $\overline{a} \cdot \overline{b} = \overline{a \cdot b} = \overline{n} = \overline{0}$. Wir erhalten Widerspruch zu Lemma 1.15. Also ist $\mathbb{Z}/n\mathbb{Z}$ kein Körper. □

Definition 3 (Charakteristik)**.** Sei K Köper. Die kleinste natürliche Zahl n mit n mal $1_K + \ldots + 1_K = 0_K$ (in K) heißt die Charakteristik von K.

Notation: char(K). Gibt es eine solche Zahl n nicht, dann setzt man char(K) = 0.

Bemerkung 4.

1. char(K) = 0 oder char(K) ≥ 2 (wegen $0_K \neq 1_K$).
2. Q, R, Chaben Charakteristik Null.
3. Z/ p Zhat die Charakteristik p.

Satz 1. char(K) ist entweder 0 oder Primzahl.

Beweis. Sei char(K) $\neq 0$, also char(K) $= n \geq 2$.

Wäre n keine Primzahl, so existieren $a, b \in \mathbb{N}, 1 < a, b < n$ mit $ab = n$. Dann gilt:

$$(1_K + \ldots + 1_K) \cdot (1_K + \ldots + 1_K) = (1_K + \ldots + 1_K) = 0.$$

Aus dem Satz vom Nullprodukt folgt $(1_K + \ldots + 1_K) = 0_K$ oder $(1_K + \ldots + 1_K) = 0_K$

Das Widerspricht der Minimalität von n. □

1.2 Homomorphismen

Definition 4. Seien $(G, *_G, e_G)$ und $(H, *_H, e_H)$ Gruppen. Eine Abbildung $f : G \to H$ heißt Gruppenhomomorphismus wenn für alle $g, g' \in G$ gilt:

$$f(g *_G g') = f(g) *_H f(g').$$