

Tutorium 4

Michael Walter

1 Ringe

1 Definition. Ein *Ring* $(R, +, \cdot)$ ist sowohl eine abelsche Gruppe $(R, +)$ als auch ein Monoid (R, \cdot) , so dass die folgenden Distributivgesetze gelten:

$$a(b + c) = ab + ac \text{ und } (a + b)c = ac + bc \quad (\forall a, b, c \in R)$$

Direkt aus der Definition folgen einige "natürliche" Rechenregeln:

2 Proposition (Rechenregeln). *Für alle $a, b \in R$ gelten:*

(i) $0a = 0$

(ii) $(-1)a = -a$

(iii) $(-a)(-b) = ab$

(iv) $(-a)b = a(-b) = -ab$

Beweis. z.B. (ii):

$$a + (-1)a = 1a + (-1)a = (1 + (-1))a = 0a \stackrel{(i)}{=} a$$

□

3 Beispiel. $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$, $(k[X], +, \cdot)$, $\{0\}$ sind Ringe. Der Nullring ist übrigens der einzige mit $1 = 0$.

Genauso z.B. der Ring $C(U)$ der stetigen Funktion auf einer Teilmenge $U \subseteq \mathbb{R}^n$ mit punktweiser Addition und Multiplikation.

4 Beispiel. Ist $(A, +)$ eine abelsche Gruppe, so bilden die Endomorphismen einen $(\text{End}((A, +)), +, \circ)$ Ring bzgl. der punktweisen Addition

$$\Phi + \Psi : a \mapsto \Phi(a) + \Psi(a)$$

und Komposition \circ .

Insbesondere erhält man so natürlich für einen Ring R dessen Endomorphismenring $\text{End}(R)$.

5 Beispiel. Beinahe ein "Spezialfall" vom letzten Beispiel sind die Matrizenringe $(k^{n \times n}, +, \cdot)$.

6 Notation. In einem beliebigen Ring schreibt man oft

$$2 := 1 + 1$$

$$3 := 1 + 1 + 1$$

...

7 Aufgabe. Sind folgende Teilmengen von \mathbb{Q} Ringe?

(i) $\mathbb{Z} + \frac{1}{2}\mathbb{Z} := \{a + \frac{1}{2}b : a, b \in \mathbb{Z}\}$

(ii) $\mathbb{Z}[\frac{1}{2}] := \{\sum_{k=0}^r \frac{a_k}{2^k} : r \in \mathbb{N}_0, a_k \in \mathbb{Z}\}$

Lösung. (i) Nein, die Menge ist nicht einmal abgeschlossen unter Multiplikation:

$$\frac{1}{2} \frac{1}{2} = \frac{1}{4} \notin \mathbb{Z} + \frac{1}{2}\mathbb{Z}$$

(ii) Ja, was man vielleicht am besten an der Darstellung

$$\mathbb{Z}[\frac{1}{2}] = \bigcup_r \frac{1}{2^r} \mathbb{Z}$$

sieht (das ist eine aufsteigende Vereinigung!). □

8 Aufgabe. Ein Ring R der nur aus idempotenten Elementen besteht (d.h. $x = x^2$ für alle $x \in R$) ist kommutativ.

Beweis. Es gelten für alle $a, b, x \in R$:

$$(a+b)^2 = a+b = a^2 + b^2 \Rightarrow ab = -ba$$

$$x = x^2 = (-x)^2 = -x$$

□

9 Definition. Ein *Teilring* S eines Rings R ist eine Untergruppe von $(R, +)$, die auch Untermonoid von (R, \cdot) ist.

10 Definition. Elemente eines Rings, die (bzgl. der Multiplikation \cdot) invertierbar sind, heißen *Einheiten*.

Die *Einheitengruppe* eines Rings R wird wie folgt definiert:

$$R^\times := \{r \in R : \exists s \in R : rs = sr = 1\}$$

11 Definition. Ein Element $0 \neq r \in R$ eines kommutativen Rings R heißt *Nullteiler*, wenn es ein $0 \neq s \in R$ gibt mit $rs = 0$.

Gibt es keine Nullteiler, so heißt der Ring *nullteilerfrei*.

12 Aufgabe. Einheiten sind keine Nullteiler.

Beweis. Annahme: $r \in R^\times$ ist Nullteiler eines kommutativen Rings R . Dann existieren $s, t \in R$ mit

$$t \neq 0 \text{ und } rs = 1 \text{ und } rt = 0$$

und es folgt ein Widerspruch:

$$t = rst = rts = 0s = 0$$

□

13 Aufgabe. Sei $R \neq \{0\}$ ein endlicher kommutativer Ring. Dann gilt:

$$R = R^\times \dot{\cup} \text{Nullteiler} \dot{\cup} \{0\}$$

Beweis. Sei $0 \neq r \in R$. Da R endlich ist existieren $m > n \in \mathbb{N}_0$ mit $r^n = r^m$, d.h.

$$0 = r^n(1 - r^{m-n})$$

Wir zeigen per Induktion über n : r ist Nullteiler oder Einheit.

IA ($n = 0$): Aus $1 = r^{m-n} = r \cdot \overbrace{r^{m-n-1}}^{\geq 0}$ folgt, dass r eine Einheit ist.

IS ($n > 0$): Betrachte

$$0 = r^n(1 - r^{m-n}) = r \cdot r^{n-1}(1 - r^{m-n})$$

Ist der rechte Faktor $r^{n-1}(1 - r^{m-n})$ nicht 0, dann ist r Nullteiler. Ansonsten wenden wir darauf die Induktionshypothese an und erhalten die Behauptung. □

14 Definition. Ein *Körper* k ist ein kommutativer Ring mit $k^\times = k \setminus 0$.

15 Korollar. Aus Aufgabe 13 folgt: Die endlichen Körper sind genau die nullteilerfreien kommutativen Ringe.

16 Aufgabe. Für welche $n \in \mathbb{N}$ ist $\mathbb{Z}/n\mathbb{Z}$ Körper?

Lösung. \bar{a} ist Nullteiler gdw. $\bar{a} \neq 0$ und es ein $\bar{b} \neq 0$ gibt mit $\bar{a}\bar{b} = 0$ gdw. $n \nmid a, n \nmid b, n \mid ab$, und das ist möglich gdw. n nicht prim ist. □

17 Definition. $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ für p prim.

18 Definition. $\Phi : R \rightarrow S$ heißt *Homomorphismus* wenn für alle $r, s \in R$ gelten:

$$\begin{aligned}\Phi(r + s) &= \Phi(r) + \Phi(s) \\ \Phi(r \cdot s) &= \Phi(r) \cdot \Phi(s) \\ \Phi(1) &= 1\end{aligned}$$

19 Proposition. Dann ist das Bild $\Phi(R)$ ein Teilring von S , und für jeden Teilring $U \subseteq S$ ist $\Phi^{-1}(U)$ ein Teilring von R .

Desweiteren gilt $\Phi(R^x) \subseteq S^x$, d.h. Φ induziert einen Gruppenhomomorphismus $\Phi|_{R^x} : R^x \rightarrow S^x$.

20 Aufgabe. Ist k ein Körper und $S \neq \{0\}$ ein Ring, dann ist jeder Homomorphismus $\Phi : R \rightarrow S$ injektiv.

Beweis. Annahme: Es existiert ein $x \neq 0$ mit $\Phi(x) = 0$. Dann gilt:

$$1 = \Phi(1) = \Phi(xx^{-1}) = \Phi(x)\Phi(x^{-1}) = 0$$

Also $S = \{0\}$. Widerspruch. \square

2 Faktoringe

21 Definition. Ein *Ideal* I ist eine Untergruppe von $I \subseteq (R, +)$ mit $RI \subseteq I$ und $IR \subseteq I$.

R heißt *einfach*, wenn nur $\{0\}$ und R Ideale sind.

22 Beispiel. Jeder Kern eines Homomorphismus ist Ideal.

23 Beispiel. Ist R ein kommutativer Ring und $a \in R$ dann ist

$$aR := \{ar : r \in R\}$$

ein Ideal, das von a erzeugte *Hauptideal*.

24 Beispiel. Spezielle für $R = \mathbb{Z}$ erkennen wir, dass Ideale in \mathbb{Z} genau die Untergruppen von $(\mathbb{Z}, +)$ sind, also die $n\mathbb{Z}$ für $n \in \mathbb{N}_0$.

25 Bemerkung. Analog zu Gruppenhomomorphismen und Normalteilern gilt: Urbilder von Idealen unter Homomorphismen sind wieder Ideale, und Bilder von Idealen unter *surjektiven* Homomorphismen sind auch wieder Ideale.

26 Aufgabe. Für einen kommutativen Ring R ist

$$I := \{a \in R : \exists n \in \mathbb{N} : a^n = 0\}$$

ein Ideal, das sogenannte *Nilradikal*.

Beweis. (1) $0 \in I$. Seien $a, b \in R$. Dann existieren $n, m \in \mathbb{N}$ mit $a^n = b^m = 0$, und es gilt:

$$\begin{aligned}(a + b)^{n+m} &= \sum_{k=0}^{n+m} \binom{n+m}{k} a^k b^{n+m-k} \\ &= \sum_{k=0}^n \binom{n+m}{k} a^k \underbrace{b^{n+m-k}}_{=0} + \sum_{k=n+1}^{n+m} \binom{n+m}{k} \underbrace{a^k}_{=0} b^{n+m-k} \\ &= 0\end{aligned}$$

Außerdem $(-a)^n = (-1)^n a^n = 0$. Also ist I eine Untergruppe von $(R, +)$.

(2) Für $r \in R$ gilt:

$$(ra)^n = r^n \underbrace{a^n}_{=0} = 0$$

Also $RI \subseteq I$, und I ist ein Ideal. \square

27 Bemerkung. In dem nichtkommutativen Ring $\mathbb{R}^{2 \times 2}$ gilt

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \in I \text{ da } \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}^2 = 0,$$

aber

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \notin I$$

Also ist I kein Ideal. Daran sieht man, dass es i.A. wirklich nötig ist, in Aufgabe 26 Kommutativität des Rings vorauszusetzen.

28 Definition. Sei $M \subseteq R$ eine beliebige Teilmenge. Das *Idealerzeugnis* von M ist definiert durch

$$\langle M \rangle_{\text{Ideal}} := \cap \{I : I \subseteq R \text{ Ideal mit } M \subseteq I\}$$

29 Bemerkung. $\langle M \rangle_{\text{Ideal}}$ ist das kleinste Ideal in R , das M enthält.

30 Aufgabe. Sei R ein kommutativer Ring, $I \subseteq R$ ein Ideal und $a \in R$. Dann gilt:

$$\langle I \cup \{a\} \rangle_{\text{Ideal}} = \{i + ra : i \in I, r \in R\}$$

Beweis. (\supseteq) ist klar. Wegen Bemerkung 29 Es genügt also zu zeigen, dass

$$M := \{i + ra : i \in I, r \in R\}$$

wirklich ein Ideal ist: Da $0 \in M$ erkennt man an

$$(i + ra) - (j + sa) = (i - j) + (r - s)a \in M,$$

dass M eine Untergruppe von $(R, +)$ ist. Und wegen

$$s(i + ra) = \underbrace{si}_{\in I} + (sr)a \in M$$

ist M sogar ein Ideal. \square

31 Definition. Ein Ideal I von R heißt *maximal*, wenn es keine echte aufsteigende Kette $I \subset J \subset R$ von Idealen in R gibt.

32 Aufgabe. Sei R ein kommutativer Ring und $I \subseteq R$ ein Ideal. Dann gilt:

$$I \text{ maximal} \Leftrightarrow \forall a \in R \setminus I : \exists b \in R : 1 - ab \in I$$

Beweis. (\Rightarrow) Sei $a \in R \setminus I$. I ist maximal, also gilt

$$\langle I \cup \{a\} \rangle_{\text{Ideal}} = R$$

Nach Aufgabe 30 lässt sich dann insbesondere die $1 \in R$ schreiben als

$$1 = i + ba$$

für gewisse $i \in I$ und $b \in R$. Also $1 - ab = i \in I$, was zu zeigen war.

(\Leftarrow) Sei $J \subseteq R$ Ideal mit $I \subset J$. Zu zeigen ist also $J = R$. Wähle ein $a \in J \setminus I \subseteq R \setminus I$. Nach Voraussetzung gibt es nun ein $b \in R$ so dass $1 - ab =: i \in I$. Folglich:

$$1 = \underbrace{i}_{\in I \subseteq J} + \underbrace{ab}_{\in J \text{ da } a \in J} \in J$$

Es gilt also tatsächlich $J = R$. \square

33 Aufgabe. Finde ein echtes Ideal $I \subset C(\mathbb{R})$ so dass gilt: Es existiert kein $x \in \mathbb{R}$ mit $f(x) = 0$ für alle $f \in I$ (vgl. ÜB 4, A 4).

Beweis. Das echte Ideal $C_c(\mathbb{R})$ aller Funktionen mit kompaktem Träger tut es. \square

34 Bemerkung. Es gilt $C_c([0, 1]) = C([0, 1])$, denn $[0, 1]$ ist ja schon kompakt. Deshalb liefert dieser Ansatz kein Gegenbeispiel zur Aufgabe auf dem Übungsblatt.

35 Definition. Sei $I \subseteq R$ ein Ideal. Dann erhält man den *Faktorring* R/I mit den Verknüpfungen

$$\begin{aligned} (r + I) + (s + I) &:= (r + s) + I \\ (r + I) \cdot (s + I) &:= (rs) + I \end{aligned}$$

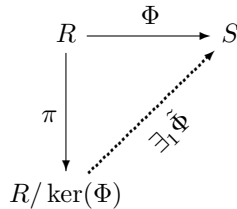
sowie einen Homomorphismus

$$\pi_I : R \rightarrow R/I, r \mapsto r + I$$

die sog. *kanonische Projektion*.

36 Bemerkung. Der Kern von π_I ist gerade I . Also sind die Ideale eines Rings R *genau* die Kerne von Homomorphismen $R \rightarrow \star$.

37 Satz (Homomorphiesatz).



und $\tilde{\Phi}$ ist injektiv.

38 Satz (Cayley).

Monoide	Gruppen
(M, \cdot) <i>Monoid</i> $\Rightarrow (\text{Abb}(M, M), \circ)$ <i>Monoid</i> $\Rightarrow L : \begin{cases} M \rightarrow \text{Abb}(M, M) \\ m \mapsto (n \mapsto mn) \end{cases}$ <i>ist injektiver Hom.</i> $\Rightarrow M \cong L(M)$	(G, \cdot) <i>Gruppe</i> $\Rightarrow (\text{Sym}(G), \circ)$ <i>Gruppe</i> $\Rightarrow L : \begin{cases} G \rightarrow \text{Sym}(G) \\ g \mapsto (h \mapsto gh) \end{cases}$ <i>ist injektiver Hom.</i> $\Rightarrow G \cong L(G)$

Ringe

$(R, +, \cdot)$ <i>Ring</i> $\Rightarrow (\text{End}((R, +)), +, \circ)$ <i>Ring</i> $\Rightarrow L : \begin{cases} R \rightarrow \text{End}((R, +)) \\ r \mapsto (s \mapsto rs) \end{cases}$ <i>ist injektiver Hom.</i> $\Rightarrow R \cong L(R)$

3 Charakteristik

39 Bemerkung. Für jeden Ring R gibt es genau einen Homomorphismus $\mathbb{Z} \rightarrow R$, nämlich

$$\Phi : \mathbb{Z} \rightarrow R, n \mapsto n \cdot 1$$

Bekanntlich hat der Kern dann die Form $\ker(\Phi) = n\mathbb{Z}$ für (genau) ein $n \in \mathbb{N}_0$.

40 Definition. $\text{char}(R) := n$ heißt *Charakteristik* von R .

41 Bemerkung. Die Charakteristik ist das kleinste $n \in \mathbb{N}$ mit

$$\underbrace{1 + \dots + 1}_{n \text{ mal}} = 0,$$

oder 0 falls es kein solches n gibt.

42 Bemerkung. Ist $R \neq \{0\}$ nullteilerfrei, dann ist die Charakteristik 0 oder prim.

43 Aufgabe. Jeder Ring von Primordnung p ist isomorph zu $\mathbb{Z}/p\mathbb{Z}$.

Beweis. Sei R ein Ring und $p := \#R$ prim. Es gilt also: $R = \langle 1 \rangle_{\text{Gruppe}}$ (Gruppen von Primordnung werden von jedem Element außer dem neutralen erzeugt). Folglich ist der Homomorphismus Φ von oben surjektiv, also $\mathbb{Z}/n\mathbb{Z} \cong R$ für ein $n \in \mathbb{N}_0$ (via Homomorphiesatz). Insbesondere gilt dann $n = \#\mathbb{Z}/n\mathbb{Z} = \#R = p$ womit die Behauptung bewiesen ist. \square