§ 5 Ringe und Körper

Auf den Zahlbereichen $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, aber auch auf $\{0,1\}$ bzw. $\{g,u\}$, sind jeweils <u>zwei</u> innere Verknüpfungen definiert. Deren Gesetzmäßigkeit wollen wir nun erfassen.
Statt $*_1$, $*_2$ schreiben wir für die beiden Verknüpfungen auch im allgemeinen Fall „+“ und „·“ (in Anlehnung an die angegebenen Beispiele).

5.1 Definition: Ring

Sei R eine Menge. Ferner seien auf R zwei innere Verknüpfungen definiert:

$$„+“ : \begin{cases} R \times R \to R \\ (a,b) \quad \mapsto a+b \end{cases} \quad \text{und} \quad „\cdot“ : \begin{cases} R \times R \to R \\ (a,b) \quad \mapsto a \cdot b =: ab \end{cases}$$

Gelten dann folgende Aussagen:

(R1) $(R,+)$ ist kommutative Gruppe (mit neutralem Element $0 \in R$);

(R2) $(R,\cdot)$ ist Halbgruppe;

(R3) die Distributivgesetze:

$\forall a,b,c \in R : (a+b)\cdot c = a\cdot c + b \cdot c$ und

$\forall a,b,c \in R : a \cdot (b+c) = a \cdot b + a \cdot c$,

dann heißt das Tripel $(R,+,\cdot)$ **Ring** (engl.: ring).

Anmerkung. 1.) Sind keine Verwechslungen (zwischen Ring und Menge) zu befürchten und ist klar, um welche Verknüpfungen es sich handelt, so schreibt man nur R statt $(R,+,\cdot)$.
2.) Oft wird (wie oben schon angegeben) der Mal-Punkt beim Produkt weggelassen.
3.) Um Klammern zu sparen, vereinbaren wir, dass die Multiplikation stärker bindet als die Addition; also z.B. $ab + c := (a \cdot b) + c$.

Beispiele.

(a) $(\mathbb{Z},+,\cdot)$, $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$, $(\mathbb{C},+,\cdot)$ sind Ringe.

(b) $(\mathbb{Z}/m\mathbb{Z},+,\cdot)$ ist für $m \in \mathbb{N}$ ein Ring, der sogenannte **Restklassenring mod m**.

Anmerkung. Ist $m \in \mathbb{N} \setminus \{1\}$ keine Primzahl, so hat $(\mathbb{Z}/m\mathbb{Z}),+,\cdot)$ sogenannte „**Nullteiler**“ (engl.: zero divisor), also Elemente $s,t \neq 0$ mit $s \cdot t = 0$. Ist z.B. $m = r \cdot s$ mit $r,s \in \mathbb{N} \setminus \{m\}$, dann gilt $\overline{r} \neq \overline{0}$, $\overline{s} \neq \overline{0}$, aber $\overline{r} \cdot \overline{s} = \overline{m} = \overline{0}$.
Insbesondere kann daher $(\mathbb{Z}_m{}^*,\cdot)$ keine Gruppe sein. *Beispiel:* $\overline{2} \cdot \overline{3} = \overline{0}$ in $(\mathbb{Z}_6,\cdot)$.

5.2 Anmerkung und Definition: Integritätsbereich

1. $(R,+,\cdot)$ heißt **nullteilerfrei**, wenn gilt

   (R4) $\forall a,b \in R : [a \cdot b = 0 \Rightarrow a = 0 \vee b = 0]$.

   Anm.: Gilt in einem Ring die Nullteilerfreiheit, so folgt die Kürzungsregel

$$\forall a, bc, d \in R : \quad ac = dc \Longrightarrow (a = d) \vee (c = 0).$$

Beweis ?

2. Ein Ring $(R, +, \cdot)$ heißt **kommutativ**, wenn $(R, \cdot)$ kommutativ ist.

3. Ein Ring $(R, +, \cdot)$ heißt **Integritätsbereich**(Integritätsring; engl.: integer domain), wenn er nullteilerfrei und kommutativ ist und mindestens zwei Elemente enthält.

Die oben unter (a) aufgeführten Beispiele von Ringen sind auch Beispiele von Integritätsbereichen; ist $m \neq 1, m \in \mathbb{N}$ keine Primzahl, so ist $\mathbb{Z}/m\mathbb{Z}$ wegen seiner Nullteiler (s. obige Anmerkung zu (b)) kein Integritätsbereich.
Beispiele von Ringen (Fortsetzung):

(c) Sei X Menge, R kommutativer Ring mit 1 (neutralem Element der Multiplikation), z.B. $R = \mathbb{R}$. Zu $f, g \in \mathrm{Abb}(X, R)$ definiert man (in Verallgemeinerung zu den Beispielen (6) zu Halbgruppen, s. §3 !):

$$f + g : \begin{cases} X \to R \\ x \ \mapsto f(x) + g(x) \end{cases} \quad \text{und} \quad f \cdot g : \begin{cases} X \to R \\ x \ \mapsto f(x) \cdot g(x) \end{cases} .$$

Dann gilt:

$(\mathrm{Abb}(X, R), +, \cdot)$ **ist ein kommutativer Ring**; dieser ist i.a. nicht nullteilerfrei. (Beweis. ...)

(d) Sei R kommutativer Ring mit 1 (z.B. $R = \mathbb{R}$). Wir definieren (mit $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$):

$\mathfrak{P}(R) := \{f \in \mathrm{Abb}(R, R) | \exists n \in \mathbb{N}_0 \exists a_0, \ldots, a_n \in R : f(x) = \sum\limits_{i=0}^{n} a_i x^i$ für alle $x \in R\}$.

Jedes Element $f \in \mathfrak{P}(R)$ heißt *Polynomabbildung*. $(\mathfrak{P}(R), +|_{\mathfrak{P}}, \cdot|_{\mathfrak{P}})$ ist ein Unterring von $(\mathrm{Abb}(R, R)+, \cdot)$. Er heißt **Ring der Polynomabbildungen von R**.

Anmerkung. Definiert man $f_a : R \to R$ durch $f_a(x) = a$ für alle $x \in R$ und $(\mathrm{id})^i : R \to R$ durch $(\mathrm{id})^i(x) = x^i$, und ist $f \in \mathfrak{P}(R)$ mit $f(x) = \sum\limits_{i=0}^{n} a_i x^i$, so gilt für alle $x \in R$:

$(\sum_{i=0}^{n} f_{a_i} \cdot (\mathrm{id}_R)^i)(x) \underset{\substack{\text{Def. + in} \\ \mathrm{Abb}(R,R)}}{=} \sum_{i=0}^{n} [f_{a_i} \cdot (\mathrm{id}_R)^i)](x) \underset{\text{Def.}}{=} \sum_{i=0}^{n} [f_{a_i}(x) \cdot (\mathrm{id}_R)^i)(x)] = \sum_{i=0}^{n} a_i x^i$.
Daher ist $f = \sum_{i=0}^{n} f_{a_i} \cdot (\mathrm{id}_R)^i$.

(d') Man kann zeigen: Die Menge $\mathbb{R}[x] := \{\sum\limits_{i=0}^{n} a_i x^i | n \in \mathbb{N}_0, a_i \in \mathbb{R}\}$ mit den Verknüpfungen

$$\sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{m} b_i x^i := \sum_{i=0}^{max(m,n)} (a_i + b_i) x^i$$

und

$$\sum_{i=0}^{n} a_i x^i \cdot \sum_{j=0}^{m} b_j x^j := \sum_{i=0}^{n} \sum_{j=0}^{m} a_i b_j x^{i+j} = \sum_{k=0}^{n+m} (\sum_{i=0}^{k} a_i b_{k-i}) x^k$$

(wobei $a_i := 0 =: b_j$ für $i > n$ und $j > m$) ist ein Ring, der reelle **Polynomring**.

(e) Sei $(G,+)$ eine abelsche Gruppe und $\mathrm{End}(G) := \{f | f : G \to G \wedge f \text{ Homomorphismus}\}$.

Definiert man für $f, g \in \mathrm{End}\, G$: $\quad f + g : x \mapsto f(x) + g(x)$
$\quad f \circ g : x \mapsto f\big(g(x)\big)$,

dann ist $(\mathrm{End}(G), +, \circ)$ ein Ring, der sogenannte **Endomorphismenring der kommutativen Gruppe G**.

5.3 Definition: Schiefkörper, Körper

Sei K Menge und seien auf K zwei innere Verknüpfungen

$$„+“ : \begin{cases} K \times K \to K \\ (a,b) \quad \mapsto a + b \end{cases} \quad \text{und} \quad „\cdot“ : \begin{cases} K \times K \to K \\ (a,b) \quad \mapsto a \cdot b (=: ab) \end{cases}$$

definiert. Für diese gelte[35]:

(K1) $(K,+)$ ist kommutative Gruppe (mit neutralem Element $0 \in K$).

(K2) $(K^*, \cdot)$ ist Gruppe[36](mit neutralem Element $1 \in K$).

(K3) die Distributivgesetze:

$\forall a,b,c \in K : (a+b) \cdot c = a \cdot c + b \cdot c$ und

$\forall a,b,c \in K : a \cdot (b+c) = a \cdot b + a \cdot c$!

Dann heißt $(K,+,\cdot)$ ein **Schiefkörper** (engl.: skew field). Gilt zusätzlich, dass $(K \backslash \{0\}, \cdot)$ kommutativ ist, so heißt $(K,+,\cdot)$ **Körper**(engl.: field).

Anmerkung. 1) Viele Autoren nennen auch Schiefkörper schon Körper und sprechen bei Körpern in unserem Sinne von kommutativen Körpern. Besondere Vorsicht ist also geboten !

2) Die besondere Bedeutung von Körpern liegt für unsere Vorlesung darin, dass die meisten Betrachtungen, die wir an (1.1) bis (1.4) anschließen wollen, nicht von spezielleren Eigenschaften der reellen Zahlen, sondern nur von ihren Körpereigenschaften abhängen. Indem wir als Skalarbereich einen beliebigen Körper zulassen, werden unsere Betrachtungen an zusätzlicher Allgemeinheit (und vielleicht auch Klarheit) gewinnen, ohne wesentlich erschwert zu werden. Unsere Betrachtungen lassen sich dann auch auf „Vektorräume“ über $\mathbb{Q}$, $\mathbb{C}$ oder $\{0,1\}$ (vgl. 1.5) anwenden.

3) Es ist auch möglich, „Vektorräume“ über Schiefkörpern (allgemein) zu definieren. Da hierbei jedoch zusätzliche Schwierigkeiten auftreten (z.B. zu unterscheiden ist, ob man vereinbart mit den Skalaren „von links“ oder „von rechts“ zu multiplizieren), werden wir in dieser Vorlesung davon absehen.

[35] mit $K^* := K \setminus \{0\}$

[36] genauer für die Verknüpfung $\cdot|_{K^*}$

5.4 Beispiele von Körpern

(a) $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$, sind Körper.

(b) $(\{0,1\}), \oplus, \odot)$ mit

$$\begin{array}{c|cc} \oplus & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array} \quad \text{und} \quad \begin{array}{c|cc} \odot & 0 & 1 \\ \hline 0 & 0 & 0 \\ 1 & 0 & 1 \end{array} \quad \text{(vgl. 1.5) ist ein Körper.}$$

(c) Für jede Primzahl p ist $\mathrm{GF}(p) := (\mathbb{Z}_p, +, \cdot) := (\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ ein Körper, das sogenannte **Galoisfeld p** (engl.: Galois field p, $\mathbb{F}_p$) (vgl. auch Bsp. (b) nach (5.1)!).

Beweis: Übungsaufgabe 5.1, s.u. !

Spezialfall: $p = 2$

Die GF(2) zugrunde liegende Menge ist:
$\mathbb{Z}_2 = \{\overline{0}, \overline{1}\}$ mit $\overline{0} = \{\ldots, -2, 0, 2, 4, \ldots\}$ und $\overline{1} = \{\ldots, -3, -1, 1, 3, \ldots\}$.

Zu den Verknüpfungen! Die Definitionen $\overline{x} + \overline{y} := \overline{x+y}$ und $\overline{x} \cdot \overline{y} := \overline{x \cdot y}$ führen zu folgenden Verknüpfungstafeln:

$$\begin{array}{c|cc} + & \overline{0} & \overline{1} \\ \hline \overline{0} & \overline{0} & \overline{1} \\ \overline{1} & \overline{1} & \overline{0} \end{array} \qquad \begin{array}{c|cc} \cdot & \overline{0} & \overline{1} \\ \hline \overline{0} & \overline{0} & \overline{0} \\ \overline{1} & \overline{0} & \overline{1} \end{array} .$$

Ein Vergleich mit den Verknüpfungstafeln des Beispiels 5.4(b) zeigt, dass die Bijektion

$$i : \begin{cases} \mathbb{Z}_2 \longrightarrow \{0,1\} \\ \overline{0} \quad \mapsto 0 \\ \overline{1} \quad \mapsto 1 \end{cases}$$

sowohl mit den Additionen auf $\mathbb{Z}_2 = \mathbb{Z}/2\mathbb{Z}$ und $\{0,1\}$ als auch mit den Multiplikationen auf diesen Mengen „verträglich“ ist.

5.5 Definition: Ring-Homomorphismus,Ring-Isomorphie

Seien $(R, +, \cdot)$ und $(S, \hat{+}, \hat{\cdot})$ Ringe. Eine Abbildung $f : R \to S$ heißt **(Ring-) Homomorphismus**, falls für alle $x, y \in R$

$$f(x+y) = f(x) \hat{+} f(y) \text{ und } f(x \cdot y) = f(x) \hat{\cdot} f(y)$$

gilt.[37] Ein bijektiver (Ring-) Homomorphismus heißt **(Ring-) Isomorphismus**.
Im Falle der Existenz eines Isomorphismus des Rings $(R, +, \cdot)$ auf den Ring $(S, \hat{+}, \hat{\cdot})$ heißen die beiden Ringe **isomorph**, in Zeichen $(R, +, \cdot) \cong (S, \hat{+}, \hat{\cdot})$, kurz $R \cong S$.

M
↓

Wie bei Gruppen, so ist auch bei Ringen die Isomorphie als eine „Strukturgleichheit“ aufzufassen. Isomorphe Ringe kann man also als „im Wesentlichen gleich“ ansehen, jedenfalls insofern man sich auf ihre Ringstruktur beschränkt.

Wie wir gleich zeigen werden, ist ein Körper ein Ring mit zusätzlichen Eigenschaften, die unter Ring-Isomorphismen erhalten bleiben. In Fortführung unseres speziellen Beispiels können wir also festhalten: i ist ein (Körper-) Isomorphismus; insbesondere gilt also:

$$(\mathbb{Z}_2, +, \cdot) \cong (\{0, 1\}, \oplus, \odot).$$

Auch im Falle von Beispiel (b) sprechen wir daher vom Galoisfeld 2. Ähnlich folgt

$$(\mathbb{Z}_2, +, \cdot) \cong (\{g, u\}, \oplus, \odot).$$

5.6 Zusammenhang Ring – Körper

$$(K, +, \cdot) \text{ ist Körper} \iff \begin{cases} (K, +, \cdot) \text{ ist kommutativer Ring mit}^{38} \quad 1 \text{ und } 1 \neq 0, \\ \text{und zu jedem Element } x \in K \setminus \{0\} \text{ existiert eine} \\ \text{multiplikative Inverse.} \end{cases}$$

Beweisskizze.

„$\Rightarrow$“ Sei $(K, +, \cdot)$ Körper. Nach Definition sind $+$, $\cdot$ innere Verknüpfungen, ist $(K, +)$ kommutative Gruppe und gelten die Distributivgesetze. Da $(K \setminus \{0\}, \cdot)$ kommutative Gruppe ist, interessiert nur noch das Verhalten von 0 bei der Multiplikation.

Sei $a \in K$. Dann folgt

$$0 \cdot a + 0 \cdot a \underset{\substack{\text{Distribut.} \\ \text{Gesetz}}}{=} (0 + 0) \cdot a \underset{\substack{\text{0 neutr.Elt} \\ \text{d.Add.}}}{=} 0 \cdot a \underset{\substack{\text{Add.v. } -(0 \cdot a) \\ \text{(ex.)} \\ \text{Assoz.-Ges. der} \\ \text{Addition}}}{\Rightarrow} 0 \cdot a = 0.$$

Analog lässt sich $a \cdot 0 = 0$ für alle $a \in K$ zeigen. Das 0-Element verletzt daher weder die Assoziativität noch die Kommutativität der Multiplikation (und es gilt $1 \cdot 0 = 0$).

Bevor wir die Rückrichtung zeigen, bemerken wir, dass bei der Herleitung von $0 \cdot a = 0 = a \cdot 0$ im oberen Beweisteil nur solche Eigenschaften benutzt wurden, die auch Ringe allgemein besitzen, und halten fest:

5.7 Hilfssatz: Produkt mit Null

In jedem Ring $(R, +, \cdot)$ gilt $0 \cdot a = 0 = a \cdot 0$ für alle $a \in R$.

Fortsetzung des Beweises von 5.6:

[37] Vgl. diese Definition mit der des Gruppen-Homomorphismus/Isomorphismus in 4.1 !

[38] wobei 1 das neutrale Element der Multiplikation bezeichnet und 0 das der Addition.

„$\Leftarrow$“ Auch hier interessiert nur noch die multiplikative Struktur.

Die Nullteilerfreiheit von K und damit die Abgeschlossenheit von $(K \setminus \{0\}, \cdot)$ erhält man dann folgendermaßen:

$$x \cdot y = 0 \wedge x \neq 0 \Rightarrow y = x^{-1}(xy) = x^{-1} \cdot 0 = 0.$$

Die zusätzlichen Eigenschaften von K bewirken, dass $(K \setminus \{0\})$ kommutative Gruppe sein muss. $\square$

5.8 Definition: Char K

Sei $(K, +, \cdot)$ Körper.

(a) Für $a \in K$ und $n \in \mathbb{N}$ definieren wir $n \cdot a := \underbrace{a + a + \cdots + a}_{n \text{ Summanden}} = (\underbrace{1 + 1 + \cdots + 1}_{n \text{ Summanden}})a = (n \cdot 1) \cdot a$ (mit $1 \in K$).

(b) Ist $m \cdot 1 \neq 0$ für alle $m \in \mathbb{N}$, so sagen wir: K hat **Charakteristik** 0; in Zeichen: $\operatorname{Char} K = 0$.

Andernfalls nennen wir die kleinste natürliche Zahl n mit $n \cdot 1 = 0$ die Charakteristik von K, in Zeichen: $\operatorname{Char} K = n$.

Beispiel. $\mathrm{GF}(p)$ hat Charakteristik p; $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ haben Charakteristik 0.

5.9 Satz: Werte von Char K

$$\boxed{K \text{ Körper} \Rightarrow \operatorname{Char} K = 0 \vee \operatorname{Char} K = p \text{ (mit geeigneter Primzahl } p).}$$

Beweis: Übungsaufgabe 5.3.

Übungsaufgaben:

Aufgabe 5.1 Sei $(R, +, \cdot)$ ein kommutativer Ring mit

$$(*) \quad x^2 = x \quad \text{für alle} \quad x \in R.$$

(Diese Eigenschaft hat z.B. jeder Potenzmengenring[39].) Zeigen Sie:
a) Für alle $x \in R$ gilt $x + x = 0$.
b) Ist $|R| > 2$, so ist $(R, +, \cdot)$ kein Integritätsbereich.
Lösungshilfe: Betrachten Sie die Terme $(a + b)^2$ und $a(a - 1)$!

Aufgabe 5.2
Zeigen Sie, dass $(\mathbb{Z}_p, +, \cdot)$ für jede Primzahl p ein Körper ist !
Lösungshinweis: Für den Nachweis der Existenz der Inversen zu $\overline{a}$ betrachtet man die injektive und damit bijektive Abbildung $\overline{x} \mapsto \overline{a} \cdot \overline{x}$.

Aufgabe 5.3 Beweisen Sie Satz 5.9 !

[39] Zur Definition des Potenzmengenringes siehe 2.2.10 und Aufgabe 5.4 !

Lösungshinweis: Zu $\operatorname{Char} K = p \cdot q$ berechnet man $(p \cdot 1)(q \cdot 1)$!

Aufgabe 5.4 Untersuchen Sie, unter welcher (notwendigen und hinreichenden) Bedingung an die nicht-leere Menge T der Potenzmengenring $(\wp(T), \triangle, \cap)$ ein Körper ist ! (Vgl. 2.2.9 d und 2.2.10 !)