1 Körper

Sie kennen bereits 2 Beispiele von Zahlkörpern:

$(\mathbb{Q}, +, \cdot)$ die rationalen Zahlen mit ihrer Addition und Multiplikation
$(\mathbb{R}, +, \cdot)$ die reellen Zahlen mit ihrer Addition und Multiplikation

Vielleicht kennen Sie auch schon

$(\mathbb{C}, +, \cdot)$ die komplexen Zahlen

Wir *definieren* nun, was wir unter einem „Körper“ verstehen, und sehen dann, dass es noch andere, ganz kleine Körper gibt:

Definition 1.1. Ein Körper ist eine Menge k, auf der 2 Operationen $+$ und $\cdot$ definiert sind, für welche die folgenden Gesetze gelten:

i)	$[\forall\, a, b, c \in k\,]\,[\,(a+b)+c = a+(b+c)\,]$	Assoziativitätsgesetz
ii)	$[\exists\, 0 \in k\,]\,[\forall\, a \in k\,]\,[\,a+0=a\,]$	Existenz eines Neutralelements
iii)	$[\forall\, a \in k\,]\,[\exists\, b \in k\,]\,[\,a+b=0\,]$	Existenz eines Inversen $(-a)$
iv)	$[\forall\, a, b \in k\,]\,[\,a+b=b+a\,]$	Kommutivitätsgesetz
v)	$[\forall\, a, b, c \in k\,]\,[\,(a\cdot b)\cdot c = a\cdot(b\cdot c)\,]$	Assoziativitätsgesetz
vi)	$[\exists\, 1 \in k\,]\,[\forall\, a \in k\,]\,[\,a\cdot 1=a\,]$	Existenz eines Neutralelements
vii)	$[\forall\, a \in k\,]\,[\,(a\neq 0) \Longrightarrow [(\exists\, b \in k\,)(a\cdot b=1)]\,]$	Existenz eines Inversen
viii)	$[\forall\, a, b \in k\,]\,[\,a\cdot b = b\cdot a\,]$	Kommutivitätsgesetz
ix)	$[\forall\, a, b, c \in k\,]\,[\,a\cdot(b+c) = (a\cdot b)+(a\cdot c)\,]$	Distributivgesetz
x)	$1 \neq 0$	Ausschluss des trivialen Beispiels

Bemerkungen:

- für das additive Inverse von a schreibt man $(-a)$ oder $-a$
- für $a+(-b)$ schreibt man meist $a-b$
- für das multiplikative Inverse von a schreibt man $\frac{1}{a}$ oder a^{-1}
- für $a\cdot\frac{1}{b}$ schreibt man manchmal auch $a:b$ oder $\frac{a}{b}$

Es gelten die folgenden Gesetzmässigkeiten:

Lemma 1.2

i) $[\forall\, a \in k\,]\,[\,0 \cdot a = 0\,]$

ii) $[\forall\, a \in k\,]\,[\,(-1) \cdot a = (-a)\,]$

iii) $[\forall\, a, b \in k\,]\,[\,a \cdot b = 0 \implies (a = 0 \vee b = 0)\,]$

Beweis

i) Es ist
$$\begin{aligned} 0 \cdot a + 1 \cdot a = (0+1) \cdot a = 1 \cdot a = a \\ 0 \cdot a + a = a \\ (0 \cdot a + a) + (-a) = a + (-a) \\ 0 \cdot a + (a + -a) = a + -a = 0 \\ 0 \cdot a + 0 = 0 \\ 0 \cdot a = 0 \end{aligned}$$

ii)
$$\begin{aligned} 0 \cdot a = 0 \\ (-1+1) \cdot a = 0 \\ (-1) \cdot a + 1 \cdot a = 0 \\ (-1 \cdot a + a) + (-a) = 0 + (-a) \\ -1 \cdot a + (a + (-a)) = (-a) \\ -1 \cdot a + 0 = -a \\ -1 \cdot a = -a \end{aligned}$$

iii) Wäre $a \neq 0$, so würde a^{-1} existieren, und

$$a \cdot b = 0 \implies a^{-1} \cdot (a \cdot b) = (a^{-1}) \cdot 0 \implies$$
$$(a^{-1} \cdot a) \cdot b = 0 \implies 1 \cdot b = 0 \implies b = 0$$

Aus $a \neq 0$ folgt also $b = 0$.

Genauso folgt aus $b \neq 0$ sofort, dass $a = 0$.

□

Wir dürfen also mit Vorzeichen, 0 und -1 genauso rechnen, wie wir es gewohnt sind. Auch die Klammern setzen wir (oder lassen sie weg), wie wir es von der Regel „Punkt vor Strich“ kennen.

Der Vollständigkeit halber beweisen wir auch noch die *Eindeutigkeit* der additiven und multiplikativen Inversen:

Lemma 1.3

Sei $(k, +, \cdot)$ ein Körper. Dann gilt

i) $[\forall\, a, b, c \in k\,]\,[\,(a + b = 0 \;\wedge\; a + c = 0) \implies b = c\,]$

ii) $[\forall\, a, b, c \in k\,]\,[\,(a \cdot b = 1 \;\wedge\; a \cdot c = 1) \implies b = c\,]$

Beweis

i) Sei also $a + b = 0$ und $a + c = 0$. Dann ist

$$\begin{aligned}
(a + b) - (a + c) &= 0 - 0 = 0 \\
a + b + (-a) + (-c) &= 0 \\
a + (-a) + b + (-c) &= 0 \\
b + (-c) &= 0 \\
b + (-c) + c &= 0 + c \\
b &= c
\end{aligned}$$

ii) Sei noch $a \cdot b = 1$ und $a \cdot c = 1$. Dann gilt

$$\begin{aligned}
a \cdot b - a \cdot c &= 1 - 1 = 0 \\
a \cdot (b - c) &= 0;\ \text{aus } a \neq 0 \text{ folgt mit Lemma 1.2 iii):} \\
b - c &= 0,\ \text{also wieder } b = c
\end{aligned}$$

□

In einem Zahlkörper (= Körper) kann man somit lineare Gleichungen genau so lösen, wie Sie es sich gewohnt sind:

Sei $a + b \cdot x = c$ gegeben mit $b \neq 0$

$$\begin{aligned}
a + b \cdot x - a &= c - a \\
a - a + b \cdot x &= c - a \qquad \big| \cdot b^{-1} \\
0 + b^{-1} \cdot b \cdot x &= b^{-1} \cdot (c - a) \\
1 \cdot x = x &= \frac{c - a}{b}
\end{aligned}$$

Die Lösung ist nach Lemma 1.3 eindeutig bestimmt.

Die Forderungen i) bis ix) der Definition 1.1 sind also eine Analyse dessen, was *mindestens* gelten muss, damit man „rechnen kann wie in $\mathbb{Q}$ oder $\mathbb{R}$“. Es sind die *Axiome* eines Körpers.

Warum bildet $(\mathbb{Z}, +, \cdot)$ *keinen* Körper ?

Definition 1.4. Zu jedem $n \in \mathbb{N}$ mit $n \geq 2$ sind die *Restklassen* bei der Division durch n als Teilmengen von $\mathbb{Z}$ definiert.

Beispiel. Für $n = 6$ gibt es 6 mögliche Reste bei der Division durch 6, nämlich 0, 1, 2, 3, 4 und 5. $\mathbb{Z}$ zerfällt in die folgenden *Restklassen modulo 6*:

$$\overline{0} = \{\ldots, \text{-12, -6, 0, 6, 12, 18}, \ldots\}$$
$$\overline{1} = \{\ldots, \text{-11, -5, 1, 7, 13, 19}, \ldots\}$$
$$\overline{2} = \{\ldots, \text{-10, -4, 2, 8, 14, 20}, \ldots\}$$
$$\overline{3} = \{\ldots, \text{-9, -3, 3, 9, 15, 21}, \ldots\}$$
$$\overline{4} = \{\ldots, \text{-8, -2, 4, 10, 16, 22}, \ldots\}$$
$$\overline{5} = \{\ldots, \text{-7, -1, 5, 11, 17, 23}, \ldots\}$$

Sprechweisen: „modulo 6 gilt $1 = 7$“ oder „es ist $-2 = 10$ modulo 6“.

Oft lässt man die Striche einfach weg, wenn klar ist, dass man von den *Restklassen* spricht.

Bezeichnung: $\mathbb{Z}_n$ bezeichnet die Menge der Restklassen in $\mathbb{Z}$ bei der Division durch n.

$\mathbb{Z}_n$ enthält n Elemente.

$$\mathbb{Z}_6 = \{\,\overline{0},\ \overline{1},\ \overline{2},\ \overline{3},\ \overline{4},\ \overline{5}\,\} \stackrel{!}{=} \{\,0,\ 1,\ 2,\ 3,\ 4,\ 5\,\}$$

Satz 1.5. Durch die folgenden Festlegungen sind 2 Operationen $+$ und $\cdot$ auf $\mathbb{Z}_n$ definiert:

i) $\overline{a} + \overline{b} := \overline{a + b}$

ii) $\overline{a} \cdot \overline{b} := \overline{a \cdot b}$

Beweis: Wir müssen zeigen, dass das Ergebnis der Definition *nicht* von der speziellen Wahl der Repräsentanten a und b für die Restklassen $\overline{a}$ und $\overline{b}$ abhängt.

Zuerst ein Beispiel in $\mathbb{Z}_6$:

Es ist $\overline{2} = \overline{8}$ und $\overline{5} = \overline{17}$ modulo 6.

$\overline{2} + \overline{5} = \overline{2 + 5} = \overline{7} = \overline{1}$, aber auch

$\overline{8} + \overline{17} = \overline{25} = \overline{1}$

Andere Repräsentanten derselben Restklassen liefern also dieselbe Summe.

In $\mathbb{Z}_n$ sind alle Repräsentanten von $\overline{a}$ von der Form $a + z \cdot n$.

i) Es ist $\overline{a} + \overline{b} = \overline{a + b}$. Für zwei beliebige Repräsentanten derselben Restklassen gilt aber auch
$\overline{a + z \cdot n} + \overline{b + y \cdot n} = \overline{a + z \cdot n + b + y \cdot n} =$
$\overline{a + b + (z + y) \cdot n} = \overline{a + b}$

ii) Genau so: $\overline{a} \cdot \overline{b} = \overline{a \cdot b}$, aber auch
$\overline{a + z \cdot n} \cdot \overline{b + y \cdot n} = \overline{(a + z \cdot n) \cdot (b + y \cdot n)} =$
$\overline{a \cdot b + a \cdot y \cdot n + b \cdot z \cdot n + y \cdot z \cdot n \cdot n} = \overline{a \cdot b}$

□

Summe und Produkt sind also eindeutig definiert, unabhängig von der speziellen Wahl der Repräsentanten für $\overline{a}$ und $\overline{b}$!

Zwei Beispiele: Wir stellen die Additions- und Multiplikationstafeln für $\mathbb{Z}_4$ und $\mathbb{Z}_5$ auf.

$\mathbb{Z}_4 +$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\mathbb{Z}_4 \cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$\mathbb{Z}_5 +$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\mathbb{Z}_5 \cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Satz 1.6. $(\mathbb{Z}_n, +, \cdot)$ genügt allen Körperaxiomen ausser vii), welches die Existenz eines multiplikativen Inversen verlangt für alle Elemente ausser 0.

Beweis: Die Multiplikationstabelle von $\mathbb{Z}_4$ zeigt, dass Axiom vii) nicht erfüllt sein muss. Dort haben nur die Elemente 1 und 3 ein multiplikatives Inverses.

Wir gehen die übrigen Axiome Punkt für Punkt durch und erkennen, dass $\mathbb{Z}_n$ das entsprechende Rechengesetz von $\mathbb{Z}$ erbt!

□

Auch $\mathbb{Z}$ ist ja *kein* Körper, weil dort nur 1 und -1 ein Inverses haben. Für alle andern Zahlen $n \neq 0$ hat $n \cdot k = 1$ *keine* Lösung in $\mathbb{Z}$.

Aber alle andern Eigenschaften besitzt $\mathbb{Z}$ und gibt sie über die Definition von $(\mathbb{Z}_n, +, \cdot)$ auch an $\mathbb{Z}_n$ weiter. Wir werden solche „Fast-Körper“ später einen „kommutativen Ring“ nennen.

Wenn wir die Multiplikationstafel von $\mathbb{Z}_5$ betrachten, stellen wir fest, dass auch vii) erfüllt ist.

$\mathbb{Z}_5$ *ist* also ein Körper!

Damit stellt sich die Frage: Für welche $n \in \mathbb{N}$ mit $n \geq 2$ ist $\mathbb{Z}_n$ ein Körper?

Satz 1.7. Für die Restklassen $\mathbb{Z}_n$ mit $+$ und $\cdot$ sind die folgenden drei Aussagen äquivalent:

i) n ist prim

ii) $\mathbb{Z}_n$ ist ein Zahlkörper

iii) $\mathbb{Z}_n$ hat keine „Nullteiler“

Beweis: Wir zeigen i) $\Longrightarrow$ ii) $\Longrightarrow$ iii) $\Longrightarrow$ i) !

i) $\Longrightarrow$ ii) Sei n also prim. Wir müssen zeigen, dass dann jedes $\overline{a} \in \mathbb{Z}_n$ mit $\overline{a} \neq \overline{0}$ ein multiplikatives Inverses besitzt.

Wir zeigen zuerst: Die n Restklassen $\overline{0} = \overline{a \cdot 0}$, $\overline{a \cdot 1}$, $\overline{a \cdot 2}$, ... , $\overline{a \cdot (n-1)}$ sind alle verschieden.

Sonst gäbe es i und j mit $0 \leq i < j < n$ und $\overline{a \cdot i} = \overline{a \cdot j}$, also $\overline{a \cdot (j-i)} = \overline{0} = \overline{n}$. Es müsste also ein $k \in \mathbb{Z}$ existieren mit

$$a \cdot (j - i) = k \cdot n$$

Die Primzahl n ist ein Teiler der Zahl $k \cdot n$, sie muss daher auch ein Teiler von a oder von $(j - i)$ sein! Dies ist aber beides nicht möglich, da sowohl $a < n$ und $j - i < n$.

Alle n Restklassen $\overline{a \cdot i}$ sind somit verschieden. Dann muss *eine* davon $\overline{1}$ sein. Sei also $\overline{a \cdot h} = \overline{1}$. Dann gilt aber $\overline{a} \cdot \overline{h} = \overline{a \cdot h} = \overline{1}$, und $\overline{h}$ ist das gesuchte multiplikative Inverse von $\overline{a}$.

ii) $\Longrightarrow$ iii) Lemma 1.2 iii)

iii) $\Longrightarrow$ i) Wir zeigen $\neg$ i) $\Longrightarrow$ $\neg$ iii) !

Ist n keine Primzahl, so existieren $a, b \in \mathbb{Z}$ mit $a \cdot b = n$. Dann gilt aber $\overline{a} \cdot \overline{b} = \overline{a \cdot b} = \overline{n} = \overline{0}$, $\mathbb{Z}_n$ enthält also Nullteiler.

□

Ist p eine Primzahl (und nur dann!), dann ist $\mathbb{Z}_p$ ein Körper mit allem drum und dran.

$$\mathbb{Z}_2,\ \mathbb{Z}_3,\ \mathbb{Z}_5,\ \mathbb{Z}_7,\ \mathbb{Z}_{11} \text{ usw. sind also } \textit{Körper}.$$

Damit haben wir schon einen schönen (aber noch unvollständigen!) Katalog von Körpern:

$$\mathbb{Q},\ \mathbb{R},\ \mathbb{C},\ \mathbb{Z}_p\ (p \text{ prim})$$

Jede lineare Gleichung hat in jedem dieser Körper eine eindeutige Lösung, wenn der Koeffizient bei der Variablen x nicht 0 ist:

Ein Beispiel in $\mathbb{Z}_7$:

$$\begin{array}{rll} 2+3\cdot x=4 & \big|+5 & \\ 3\cdot x=2 & \big|\cdot 5 & (3^{-1}=5) \\ 15\cdot x=10 & \text{also} & \\ 1\cdot x=3 & \text{somit} & \underline{\underline{x=3}} \end{array}$$

(alle Rechnungen modulo 7)

Test: $2+3\cdot 3=2+9=11=4$

Einige kleine Aufgaben:

1. Betrachten Sie $2+3\cdot x=4$ als Gleichung in $\mathbb{Z}_5$ und bestimmen Sie *die* Lösung!

2. In $\mathbb{Z}_{23}$: Finden Sie einfache Repräsentanten für -17 und $\frac{1}{17}$.

3. Wie findet man allgemein die additive Gegenzahl zu a in $\mathbb{Z}_n$?

4. Bestimmen Sie 18^{-1} und 19^{-1} in $\mathbb{Z}_{47}$. (47 ist prim)

5. Bestimmen Sie 18^{-1} und 19^{-1} in $\mathbb{Z}_{241}$. (241 ist prim)

6. Berechnen Sie von Hand das Produkt von 51 und 67 und prüfen Sie Ihre Rechnung mit der Siebenerprobe.

7. Sei p eine Primzahl. Wie kann man allgemein a^{-1} bestimmen in $\mathbb{Z}_p$? (schwierig!)

8. Wie viele Primzahlen gibt es überhaupt?

   Welches ist die grösste?

   Was bedeutet das für die Probleme 4. – 6. ?!

9. Sie kennen alle die Darstellung von $\mathbb{Z}$ als unendliche Punktreihe auf der Zahlengeraden. Wie könnte man sich entsprechend $\mathbb{Z}_5$ oder $\mathbb{Z}_6$ vorstellen?

Neunerprobe und Rechnen modulo 9

Sie kennen alle die Neunerprobe beim Multiplizieren, Dividieren oder auch beim Addieren:

$$\begin{array}{ccccc} 13 & \cdot & 8 & = & 104 \\ \downarrow & & \downarrow & & \downarrow \\ 4 & \cdot & 8 & = & 5 \end{array} \qquad 4 \cdot 8 = 32 \stackrel{!}{=} 5 \bmod 9$$

Also **kann** das Resultat stimmen!

2. Beispiel:

$$\begin{array}{ccccc} 76 & \cdot & 84 & = & 6384 \\ \downarrow & & \downarrow & & \downarrow \\ 13 & & 12 & & 21 \\ \downarrow & & \downarrow & & \downarrow \\ 4 & \cdot & 3 & \stackrel{?}{=} & 3 \end{array} \qquad 4 \cdot 3 = 12 \stackrel{!}{=} 3 \bmod 9$$

Man bildet die „einstellige Quersumme“ und prüft, ob für **diese** die Rechnung **mod 9** stimmt!

Behauptung: Das Bilden der „einstelligen Quersumme“ bedeutet einfach, die Rechnung auf $\mathbb{Z}_9$ zu übertragen, also $\overline{76} \cdot \overline{84}$ mod 9 zu prüfen.

Beweis

1. Die Stellen auf ihre Ziffern reduzieren:

$$\begin{aligned} 300 \bmod 9 = 3 \cdot 100 \bmod 9 = 3 \cdot 1 \bmod 9 &= 3 \\ 60 \bmod 9 = 6 \cdot 10 \bmod 9 = 6 \cdot 1 \bmod 9 &= 6 \\ 7 \bmod 9 &= 7 \end{aligned}$$

   9, 99, 999, 9999 usw. sind alle $= 0 \bmod 9$!!

2. Die Quersumme bilden:

$$\begin{aligned} (300 + 60 + 7) \bmod 9 = & \qquad \text{Satz 1.5 i) !!} \\ (3 + 6 + 7) \bmod 9 = 16 \bmod 9 = 7 & \end{aligned}$$

□

Bemerkung: Stimmt die Rechnung $a \cdot b = c$, dann muss sie auch „modulo 9“ stimmen: $\overline{a} \cdot \overline{b} = \overline{c}$, wobei sich $\overline{a}$, $\overline{b}$ und $\overline{c}$ durch die „einstellige Quersumme“ bestimmen lassen.

Aber: Stimmt die Neunerprobe, so muss die Rechnung noch lange nicht stimmen!

Beispiel:

$$\begin{array}{ccccc} 13 & \cdot & 8 & = & 122 \\ \downarrow & & \downarrow & & \downarrow \\ 4 & \cdot & 8 & & 5 \end{array}$$

$$4 \cdot 8 = 32 = 5 \bmod 9$$

Zum richtigen Resultat können beliebige Vielfache von 9 addiert oder subtrahiert werden.

Auch für sehr grosse Primzahlen p ist es sehr leicht, die additive Gegenzahl in $\mathbb{Z}_p$ zu finden: $a + (p - a) = 0$.

Anders ist es mit dem multiplikativen Inversen! Bei kleineren Primzahlen (sagen wir $< 10\,000$) findet der TR mit einer for-Schleife noch schnell die Zahl b mit $a \cdot b = 1$ modulo p. Dieses „Durchprobieren“ wird aber bald sehr langsam, wenn p gross wird. Zum Glück gibt es aber eine **wesentlich** schnellere Methode. Diese ist der Inhalt des nächsten Abschnittes.