$-(0 \cdot a)$ addieren.

Das ergibt

$$0 = 0 \cdot a - 0 \cdot a = 0 \cdot a.$$

Propo 3.16 Sei R ein Ring. Dann gilt für alle $a \in R$

$$(-1) \cdot a = -a = a \cdot (-1)$$

Beweis Übungsaufgabe.

Propo 3.17 Sei R ein Ring. Dann ist R der Nullring genau dann, wenn $0 = 1$.

Beweis Falls R Nullring, so gilt $0 = 1$.
Nehmen wir also an, $0 = 1 \in R$.
Wir müssen also jetzt zeigen, daß $R = \{0\}$.
Sei hierfür $a \in R$ beliebig.
Es gilt

$$a \cdot 1 = a \overset{3.15}{=} a \cdot 0 = 0$$

Also $a = 0$, d.h. $R = \{0\}$.

Wie bei Gruppen zeigt man:

Propo 3.18 Sei R ein Ring und $1'$ und 1 neutrale Elemente bezüglich der Multiplikation, so gilt $1' = 1$.

Beweis Nach (R3) gilt $a \cdot 1 = a = 1 \cdot a$ und $1' \cdot b = b = b \cdot 1'$ für alle $a, b \in R$. Insbesondere gilt für $a = 1'$ und $b = 1$: $1' \cdot 1 = 1' = 1$. □

Ein Ring $(R, +, \cdot)$ in dem $a \cdot b = b \cdot a$ für $a, b \in R$ heißt kommutativer Ring.

Bsp 3.19 Offenbar sind $R = \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ mit Verknüpfungen „+" und „·" Ringe. Da $a \cdot b = b \cdot a$ für $a, b \in R$ sind diese Ringe auch kommutativ.

Wir erinnern an die kommutative Gruppe $(\mathbb{Z}/n\mathbb{Z}, +)$. Diese Gruppe können wir durch weitere Verknüpfung

$[a] \cdot [b]$ = Rest von $a \cdot b$

zu einem Ring $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ machen.

Da $(\mathbb{Z}/n\mathbb{Z}, +)$ bereits kommutative Gruppe ist, müssen wir nur noch (R2), (R3) und (R4) nachprüfen.

Zu (R3): Für $[1] \in \mathbb{Z}/n\mathbb{Z}$ gilt:

$[a] \cdot [1]$ = Rest von a = $[a]$

$[1] \cdot [a]$ = Rest von a = $[a]$

Wegen Propo. 3.18 gilt

$\underline{1} = [1]$.

Analog zeigt man (R2) und (R4).

Der Ring $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ ist kommutativ. Es gilt nämlich

$[a][b]$ = Rest $a \cdot b$ = Rest $b \cdot a$ = $[b][a]$.

Wir werden später Ringe kennenlernen, die nicht kommutativ sind.

*

§ 4
Körper

In den Ringen $(\mathbb{Q}, +, \cdot)$ und $(\mathbb{R}, +, \cdot)$ existiert für jedes Element $a \neq 0$ ein Inverses bezüglich „$\cdot$". In dem Ring $(\mathbb{Z}, +, \cdot)$ hingegen nicht.

(Um lineare Gleichungssysteme zu lösen, reicht es nicht Ringe als Zahlenmengen zu betrachten. Zum Beispiel ist die Gleichung

$$3x - 7 = 0$$

im Ring $(\mathbb{Z}, +, \cdot)$ nicht lösbar. In $\mathbb{Q}$ oder $\mathbb{R}$ allerdings schon. Bei Gleichungen der Form $aX + b = 0$, $a \neq 0$ müssten wir Folgende Umformung machen können:

$$aX + b = 0 \text{ , also } aX = -b.$$

Wenn in der Zahlenmenge das Inverse zu a bezüglich „$\cdot$" existiert, erhält man

$$x = -b \cdot a^{-1} = -\frac{b}{a}$$

als Lösung. Dies führt auf den Begriff „Körper".

Def 4.1 Sei K ein kommutativer Ring. Man nennt K einen Körper, wenn gilt:

(i) $1 \neq 0$

(ii) jedes Element $a \neq 0$ besitzt ein Inverses bezüglich „$\cdot$".

Bsp. 4.2 offenbar sind $(\mathbb{Q}, +, \cdot)$ und $(\mathbb{R}, +, \cdot)$ Körper.

Propo 4.3 Sei K ein Körper und $a, a', b \in K$ mit $b \neq 0$. Wenn $ab = a'b$, dann $a = a'$

Beweis Multiplizieren $ab = a'b$ auf beiden Seiten mit b^{-1}. □

Propo 4.4 Sei K ein Körper und $a, b \in K$. mit $ab = 0$. Dann ist $a = 0$ oder $b = 0$.

Beweis $ab = 0$, $a \neq 0$. Dann $a^{-1}ab = b = 0$. ⊡

Wir wollen unsere $(\mathbb{Q}, +, \cdot)$ und $(\mathbb{R}, +, \cdot)$ weitere Beispiele von Körpern angeben.

Wir führen nun den Körper der komplexen Zahlen $\mathbb{C}$ ein.

Wir setzen

$$\mathbb{C} := \mathbb{R} \times \mathbb{R} = \{(a, a') \mid a, a' \in \mathbb{R}\}$$

und definieren Addition und Multiplikation durch

$$(a, a') + (b, b') = (a + b, a' + b')$$
$$(a, a') \cdot (b, b') = (ab - a'b', ab' + a'b)$$

Man prüft leicht nach, dass $(\mathbb{C}, +)$ eine kommutative Gruppe ist. Das neutrale Element ist $0 = (0, 0)$ und das Negative von (a, a') ist $(-a, -a')$.

Außerdem prüft man leicht nach, daß $(\mathbb{C}, +, \cdot)$ ein kommutatives Ring ist.

Das Einselement ist $1 = (1,0)$ und

$$0 = (0,0) \neq (1,0) = 1.$$

Das entscheidende noch zu zeigende ist:

Propo 4.5 Das Inverse zu $(0,0) \neq (a,a') \in \mathbb{C}$ ist

$$(a,a')^{-1} = \left(\frac{a}{a^2+a'^2} , \frac{-a'}{a^2+a'^2} \right)$$

Beweis Nachrechnen.

Wir sehen, $(\mathbb{C}, +, \cdot)$ ist Körper. Nullelement ist $0 = (0,0)$ und Einselement ist $1 = (1,0)$.

Das Element $(0,1) \in \mathbb{C}$ heißt imaginäre Zahl und wird mit i bezeichnet.

Es gilt

$$i^2 = (0,1) \cdot (0,1) = (-1,0) = -1$$

Dafür schreibt man auch $i = \sqrt{-1}$.

Da -1 in $\mathbb{R}$ kein Quadrat ist, heißt i „imaginär".

Es gilt jetzt:

$$(a,a') = (a,0) + (0,1)\cdot(a',0) = a\cdot 1 + a'\cdot 1\cdot i$$
$$= a + i\cdot a'$$

Wir schreiben komplexe Zahlen $z = (a,a') \in \mathbb{C}$ daher auch als $z = a + ia'$.

Def 4.6 Sei $z = a + ia' \in \mathbb{C}$ eine komplexe Zahl, so heißt a der Realteil und a' der Imaginärteil der Zahl z. Das komplex Konjugierte von $z = a + ia'$ ist $\overline{z} = a - ia'$.
Der Betrag von z ist $|z| = \sqrt{a^2 + a'^2}$.

Mit $i^2 = -1$ ergeben die Verknüpfungen

$$(a + ia') + (b + ib') = (a+a') + i(b+b')$$

$$(a + ia')\cdot(b + ib') = (aa' - bb') + i(ab' + ba')$$

Betrachten wir die Gleichung

$$\text{(*)} \qquad x^2 + 1 = 0 \,,$$

so sehen wir $\Delta = 0 - 4 = -4$. Die Zahl -4 ist kein Quadrat in $\mathbb{R}$. Daher hat (*) in $\mathbb{R}$ keine Lösung. In $\mathbb{C}$ jedoch gilt

$$(2i)^2 = -4 .$$

Also hat (*) in $\mathbb{C}$ die Lösungen $\pm i$.

Dies kann man verallgemeinern zu

Theorem 4.7 (Fundamentalsatz der Algebra)

Jede Gleichung

$$a_n x^n + a_{n-1} x^{n-1} + \dots + a_0 = 0$$

mit $n \geq 1$ und $a_0, \dots, a_n \in \mathbb{C}$, $a_n \neq 0$ hat eine Lösung in $\mathbb{C}$.

Beweis wird in Analysis IV geführt.

Wir haben gesehen, daß $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ ein kommutativer Ring ist.

Für $n = 2$ gilt

$+$	$[0]$	$[1]$
$[0]$	$[0]$	$[1]$
$[1]$	$[1]$	$[0]$

$\cdot$	$[0]$	$[1]$
$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$

Offenbar hat $[1]$ ein Inverses. Also ist $\mathbb{Z}/2\mathbb{Z}$ ein Körper.

Man kann auch $n = 3$ betrachten:

$\cdot$	$[0]$	$[1]$	$[2]$
$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$
$[2]$	$[0]$	$[2]$	$[1]$

Wir sehen, daß $[1]$ und $[2]$ ein Inverses besitzen. Also ist auch $\mathbb{Z}/3\mathbb{Z}$ ein Körper.

Für $n = 4$ allerdings gilt:

$$[2] \cdot [2] = [0]$$

Mit Proposition 4.4 folgt dann aber, daß $\mathbb{Z}/4\mathbb{Z}$ kein Körper ist.
Es stellt sich die Frage, für welche $n \geq 1$ der Ring $\mathbb{Z}/n\mathbb{Z}$ ein Körper ist.
Wir müssen schauen, für welche $n \geq 1$ die Elemente $[a] \neq [0] \in \mathbb{Z}/n\mathbb{Z}$ ein Inverses besitzen.

Propo 4.8 Sei $[0] \neq [a] \in \mathbb{Z}/n\mathbb{Z}$. Dann besitzt $[a]$ ein Inverses genau dann, wenn ein $b \in \mathbb{Z}$ existiert mit der Eigenschaft, daß n die Zahl $ab-1$ teilt.

Beweis Sei $[b]$ das Inverse zu $[a]$.
Dann gilt

$[a] \cdot [b] =$ Rest von $a \cdot b = [1]$.

Also $a \cdot b = q \cdot n + 1$, oder
$a \cdot b - 1 = q \cdot n$. Also existiert ein $b \in \mathbb{Z}$, so daß n die Zahl $ab-1$ teilt.