universität
innsbruck
Institut für Mathematik

Elementare Algebra und Zahlentheorie

Tim Netzer

Inhaltsverzeichnis

Kapitel 1

Wichtige Zahlbereiche

Die Mathematik ist eine Art Spielzeug, welches die Natur uns zuwarf zum Troste und zur Unterhaltung in der Finsternis.

Jean-Baptist le Rond d'Alembert (1717-1783)

Im ersten Teil der Vorlesung sollen wichtige mathematische Zahlbereiche vorgestellt werden. Dabei handelt es sich um Mengen, in denen mathematische Operationen wie Addition und Multiplikation definiert sind. Die Zahlentheorie beschäftigt sich mit der Untersuchung dieser Bereiche. Häufig wird dabei nach der Lösbarkeit von Gleichungen gefragt. Wir werden grundlegende Methoden und Ergebnisse der elementaren Zahlentheorie kennenlernen.

1.1 Die ganzen Zahlen $\mathbb{Z}$

Die ganzen Zahlen hat der liebe Gott gemacht, alles andere ist Menschenwerk
Leopold Kronecker (1823-1891)

1.1.1 Eigenschaften

Die *ganzen Zahlen* sind eine der wichtigesten Grundstrukturen der Zahlentheorie und der ganzen Mathematik. Es handelt sich dabei um die unendliche Menge

$$\mathbb{Z} = \{\ldots -3, -2, -1, 0, 1, 2, 3 \ldots\}.$$

Wir wollen die Existenz der ganzen Zahlen als gegeben annehmen (obwohl man sie auch konstruieren kann). Für zwei ganze Zahlen a und b ist ihre Summe $a + b$ und ihr Produkt $a \cdot b$ wieder eine ganze Zahl. Die Menge $\mathbb{Z}$ ist also mit einer Addition $+$ und einer Multiplikation $\cdot$ versehen. Formal handelt es sich dabei um *zweistellige Verknüpfungen*, also Abbildungen

$$+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$$
$$\cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$$

Dabei bezeichnet $\mathbb{Z} \times \mathbb{Z}$ das karthesische Produkt, also die Menge aller geordneten Paare ganzer Zahlen:

$$\mathbb{Z} \times \mathbb{Z} = \{(a, b) \mid a, b \in \mathbb{Z}\}.$$

Es gibt in $\mathbb{Z}$ nun (mindestens) zwei ausgezeichnete Elemente, nämlich 0 und 1. Die besondere Eigenschaft der 0 ist die *Neutralität bezüglich Addition*, d.h. es gilt $a + 0 = a$ für alle $a \in \mathbb{Z}$. Die Zahl 1 hat die gleiche Eigenschaft bezüglich der Multiplikation, d.h. es gilt $a \cdot 1 = a$ für alle $a \in \mathbb{Z}$. Eine weitere wichtige Eigenschaft ist die *Existenz von additiv inversen Elementen*, d.h. für jedes $a \in \mathbb{Z}$ existiert ein $b \in \mathbb{Z}$ mit $a + b = 0$. *Multiplikativ inverse Elemente* exisitieren im allgemeinen nicht, d.h. es gibt nicht für jedes $a \in \mathbb{Z}$ ein $b \in \mathbb{Z}$ mit $a \cdot b = 1$.
Wir fassen diese und weitere wichtige Eigenschaften der ganzen Zahlen in der folgenden Liste zusammen.

$\forall a, b$	$a + b = b + a$	(Kommutativität von $+$)	(1.1)
$\forall a, b, c$	$(a + b) + c = a + (b + c)$	(Assoziativität von $+$)	(1.2)
$\forall a$	$a + 0 = a$	(Additiv neutrales Element)	(1.3)
$\forall a\, \exists b$	$a + b = 0$	(Additiv inverse Elemente)	(1.4)
$\forall a, b$	$a \cdot b = b \cdot a$	(Kommutativität von $\cdot$)	(1.5)
$\forall a, b, c$	$(a \cdot b) \cdot c = a \cdot (b \cdot c)$	(Assoziativität von $\cdot$)	(1.6)
$\forall a$	$1 \cdot a = a$	(Multiplikativ neutrales Element)	(1.7)
$\forall a, b, c$	$a \cdot (b + c) = a \cdot b + a \cdot c$	(Distributivgesetz)	(1.8)

Dabei setzen wir ab jetzt immer voraus, dass $\cdot$ stärker bindet als $+$. Die rechte Seite der letzten Zeile ist also wie $(a \cdot b) + (a \cdot c)$ zu lesen.
Viele weitere Eigenschaften der ganzen Zahlen können wir bereits aus diesen 8 Eigenschaften ableiten. Später werden wir deshalb auch *axiomatisch* arbeiten,

d.h. nur mit gegebenen Eigenschaften operieren, und nicht mit expliziten Zahlbereichen wie $\mathbb{Z}$. Einige solche Beweise wollen wir aber bereits jetzt nur für die ganzen Zahlen anschauen.

Lemma 1.1.1. *Für jedes $a \in \mathbb{Z}$ gibt es genau ein $b \in \mathbb{Z}$ mit $a + b = 0$.*

Beweis. Die Existenz eines solchen b ist Eigenschaft (1.4). Um die Eindeutigkeit zu zeigen nehmen wir an, dass ein $b' \in \mathbb{Z}$ ebenfalls $a + b' = 0$ erfüllt. Nun gilt

$$b = b + 0 = b + (a + b') = (b + a) + b' = (a + b) + b' = 0 + b' = b' + 0 = b'.$$

Damit ist die Eindeutigkeit gezeigt. Man beachte, dass wir dabei die Eigenschaften (1.1),(1.2) und (1.3) mehrfach benutzt haben. □

Da das additiv inverse Element zu gegebenem a eindeutig bestimmt ist, werden wir es in Zukunft mit $-a$ (statt wie bisher mit b) bezeichnen. Wir werden auch $c - d$ schreiben, und damit $c + (-d)$, also *„c plus das additiv inverse Element zu d"* meinen. Wir können also beliebige Elemente von anderen *abziehen*. Weitere bekannte Aussagen sind die folgenden:

Lemma 1.1.2. *Es gilt $a \cdot 0 = 0$ für alle $a \in \mathbb{Z}$.*

Beweis. Es gilt

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

Zieht man nun auf beiden Seiten das Element $a \cdot 0$ ab (d.h. man addiert sein additiv Inverses auf beiden Seiten; dabei entsteht 0), so erhält man

$$0 = a \cdot 0 + 0 = a \cdot 0.$$

Genau das war zu zeigen. □

Lemma 1.1.3. *Es gilt $(-1) \cdot (-1) = 1$.*

Beweis. Es gilt

$$\begin{aligned} 1 &= 1 + 0 \cdot (-1) \\ &= 1 + (1 + (-1)) \cdot (-1) \\ &= 1 + 1 \cdot (-1) + (-1) \cdot (-1) \\ &= 1 + (-1) + (-1) \cdot (-1) \\ &= 0 + (-1) \cdot (-1) \\ &= (-1) \cdot (-1). \end{aligned}$$

Dabei haben wir gleich in der ersten Zeile Lemma 1.1.2 benutzt, und im weiteren immer wieder verschiedene der Eigenschaften (1.1)-(1.8). Insbesondere haben wir teilweise auch Klammerung weggelassen, was durch das Assoziativitätsgesetz gerechtfertigt ist. □

Die ganzen Zahlen haben eine weitere wichtige Eigenschaft, die nicht aus den Eigenschaften (1.1)-(1.8) abgeleitet werden kann. Das ist die sogenannte *Nullteilerfreiheit*:

$$a \cdot b = 0 \Rightarrow a = 0 \text{ oder } b = 0.$$

Aus dieser Eigenschaft folgt auch die Kürzungsregel:

Lemma 1.1.4. *Falls $a \neq 0$ und $ab = ac$, so gilt $b = c$.*

Beweis. Aus $ab = ac$ folgt $0 = ab - ac = a(b - c)$. Da $a \neq 0$ folgt aus der Nullteilerfreiheit $b - c = 0$ und daraus $b = c$. □

Man beachte dass wir keineswegs einfach durch a geteilt haben. In den ganzen Zahlen ist das ja auch im Allgemeinen nicht möglich, und man müsste zunächst die rationalen Zahlen kennen oder konstruieren. Das haben wir aber hier nicht getan!

1.1.2 Teilbarkeit in $\mathbb{Z}$

Definition 1.1.5. Seien $a, b \in \mathbb{Z}$. Wir nennen a einen *Teiler von* b, falls ein $c \in \mathbb{Z}$ existiert mit $a \cdot c = b$. Wir schreiben dafür auch $a|b$ („*a teilt b*").

Beispiel 1.1.6. 3 ist ein Teiler von 12, -2 ist ein Teiler von 4 und 18 ist ein Teiler von -36.

Das folgende leichte Lemma werden wir in Zukunft immer wieder (ohne Verweis) verwenden:

Lemma 1.1.7. *Falls $a|b$ und $a|c$, so auch*

$$a|(n \cdot b + m \cdot c)$$

für alle $n, m \in \mathbb{Z}$.

Beweis. Falls $a \cdot x = b$ und $a \cdot y = c$, so

$$n \cdot b + m \cdot c = n \cdot a \cdot x + m \cdot a \cdot y = (n \cdot x + m \cdot y) \cdot a.$$

Dabei haben wir das Kommutativ- und das Distributivgesetz verwendet. □

Definition 1.1.8. Seien $a \neq 0, b \neq 0$ ganze Zahlen. Eine positive Zahl $d \in \mathbb{Z}$ heißt größter gemeinsamer Teiler von a und b, falls gilt

(i) $d|a$ und $d|b$

(ii) Falls $c|a$ und $c|b$ für ein $c \in \mathbb{Z}$, so folgt $c|d$.

Nach dieser Definition stellt sich nun die Frage, ob ein größter gemeinsamer Teiler für je zwei Zahlen $a, b \in \mathbb{Z}$ existiert, ob er eindeutig bestimmt ist, und wie man ihn gegebenenfalls berechnen kann. Diese Fragen wollen wir im folgenden untersuchen. Zunächst die Eindeutigkeit:

Lemma 1.1.9. *Zwei Zahlen $a, b \in \mathbb{Z}$ haben höchstens einen größten gemeinsamen Teiler.*

Beweis. Seinen d, d' positive ganze Zahlen, die beide die Eigenschaften (i) und (ii) aus Definition 1.1.8 erfüllen. Weil d (i) und d' (ii) erfüllt folgt $d|d'$. Ganz analog folgt $d'|d$. Da d und d' aber beide positiv sind folgt $d = d'$. □

Wir bezeichnen von nun an den eindeutig bestimmten größten gemeinsamen Teiler zweier Zahlen a, b mit $\mathrm{ggT}(a, b)$, falls er existiert. In der Tat existiert er immer. Um das zu beweisen verwenden wir im nächsten Abschnitt den Euklidischen Algorithmus. Er basiert auf der Division mit Rest:

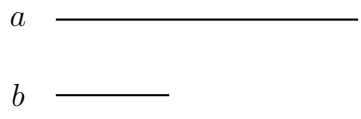
Division mit Rest. *Seien $a, b \in \mathbb{Z}$ und $b \neq 0$. Dann gibt es ganze Zahlen n, r mit*

$$a = n \cdot b + r$$

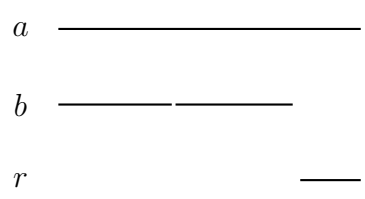
und $0 \leq r < |b|$. Dabei heißt r der Rest bei Division von a durch b.

1.1.3 Der Euklidische Algorithmus

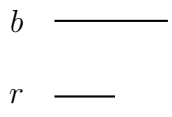
Der Euklidische Algorithmus war ursprünglich eine geometrische Methode der Griechen, um das Längenverhältnis zweier Strecken zu bestimmen. Dabei gingen sie wie folgt vor. Gegeben seien zwei Strecken a und b:



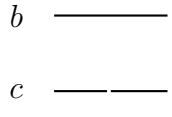
Im ersten Schritt wird die Strecke b so oft wie möglich voll in a abgetragen. Der Rest wird mit r bezeichnet. Es handelt sich dabei also genau um Teilung mit Rest:



Da r kürzer als b ist, kann die Prozedur nun mit b anstelle von a und r anstelle von b wiederholt werden:



Wenn die Prozedur nach endlich vielen Schritten aufgeht, haben wir eine Einheit gefunden, in der wir sowohl a als auch b ausdrücken können. Es wird also ein gemeinsamer Teiler beider Strecken produziert. Hier zum Beispiel nehmen wir an dass r genau 2 mal in b passt:



Es ist also $b = 2r$, und weil ursprünglich $a = 2b + r$ galt, finden wir $a = 5r$. In der Einheit r lässt sich also sowohl a als auch b ganzahlig ausdrücken, und das Verhältnis von a zu b war also genau 5 zu 2. Im Allgemeinen wird die Prozedur mehr als zwei Schritte erfordern. Trotzdem kann man durch Rückeinsetzung die ursprünglichen Strecken in der letzten erhaltenen Strecke ausdrücken. Dieser Algorithmus wird der *Euklidische Algorithmus* genannt, und wir formalisieren ihn nun für beliebige Elemente $a, b \in \mathbb{Z}$.

Euklidischer Algorithmus. *(i) Der Algorithmus erhält als Eingabe zwei positive ganze Zahlen a, b mit $b \leq a$.*

(ii) Es wird Teilung mit Rest auf a und b angewandt:

$$a = nb + r$$

mit $n \in \mathbb{Z}$ und $0 \leq r < b$.

(iii) Falls $r = 0$, so wird b als Ergebnis ausgegeben. Falls $r > 0$ so wird Schritt (ii) wiederholt, diesmal mit b anstelle von a und r anstelle von b.

Beispiel 1.1.10. Wir wenden den Algorithmus auf die Zahlen $a = 17$ und $b = 3$ an. Im ersten Schritt berechnen wir

$$17 = 5 \cdot 3 + 2.$$

Da der Rest 2 und nicht 0 ist, wiederholen wir den Vorgang, diesmal mit $a = 3$ und $b = 2$. Wir erhalten

$$3 = 1 \cdot 2 + 1.$$

Wiederum bleibt ein Rest von 1, also wiederholen wir ein drittes Mal:

$$2 = 2 \cdot 1 + 0.$$

Da nun kein Rest mehr bleibt, geben wir die letzte Zahl b, hier die 1, als Ergebnis aus. Man sieht, dass sich 17 und 3 als ganzzahlige Vielfache des Ergebnisses 1 ausdrücken lassen.

Beispiel 1.1.11. Wir wenden den Euklidischen Algorithmus auf die Zahlen $a = 118$ und $b = 24$ an. Die einzelnen Schritte sind dabei wie folgt:

$$118 = 4 \cdot 24 + 22$$

$$24 = 1 \cdot 22 + 2$$

$$22 = 11 \cdot 2 + 0.$$

Wir erhalten als Ausgabe also die Zahl 2. Wiederum lassen sich 118 und 24 als Vielfache von 2 ausdrücken.

Es stellt sich nun heraus, dass der Euklidische Algorithmus nicht nur einen gemeinsamen Teiler der Zahlen a und b produziert, sondern sogar den größten gemeinsamen Teiler:

Satz 1.1.12. *Der Euklidische Algorithmus bricht bei jeder Eingabe zweier positiver ganzer Zahlen a und b nach endlich vielen Schritten ab. Die Ausgabe ist gerade der größte gemeinsamen Teiler $\mathrm{ggT}(a, b)$. Insbesondere haben je zwei ganze Zahlen einen größten gemeinsamen Teiler.*

Beweis. Der Rest r wird in jedem Schritt strikt kleiner. Also wird nach endlich vielen Schritten $r = 0$ erreicht. Damit bricht der Algorithmus ab.
Wir zeigen dass der Algorithmus gerade $\mathrm{ggT}(a, b)$ ausgibt mit Induktion über die Anzahl der Schritte bis zum Abbruch.

Induktionsanfang: Dass der Algorithmus bereits nach dem ersten Schritt abbricht bedeutet gerade $a = n \cdot b + 0$, d.h. $b|a$. In diesem Fall ist aber offensichtlich $b = \mathrm{ggT}(a, b)$, und das ist auch genau die Ausgabe des Algorithmus.
Induktionsannahme: Falls der Algorithmus nach N Schritten abbricht, ist die Ausgabe der größte gemeinsame Teiler von a und b.
Induktionsschritt: Der Algorithmus für breche bei Eingabe von a und b genau nach $N + 1$ vielen Schritten ab. Schreibe

$$a = n \cdot b + r \tag{1.9}$$

mit $0 < r < b$ und setze $a_2 = b, b_2 = r$. Dann bricht der Algorithmus für a_2 und b_2 nach genau N Schritten ab, und gibt nach Induktionsvoraussetzung gerade $\mathrm{ggT}(a_2, b_2)$ aus. Es reicht also zu zeigen dass der größte gemeinsame Teiler von a_2, b_2 auch der größte gemeinsame Teiler von a, b ist.
Aus 1.9 sieht man aber, dass jeder Teiler von a und b auch ein Teiler von r, und also ein Teiler von a_2 und b_2 ist. Umgekehrt ist jeder Teiler von $a_2(= b)$ und $b_2(= r)$ auch ein Teiler von a (und b). Somit haben die Paare (a, b) und (a_2, b_2) genau die gleichen gemeinsamen Teiler. Da $\mathrm{ggT}(a_2, b_2)$ aber existiert, ist er damit identisch zu $\mathrm{ggT}(a, b)$.
Wenn schließlich aber je zwei positive ganze Zahlen einen ggT besitzen, so auch je zwei ganze Zahlen. Offensichtlich gilt ja $\mathrm{ggT}(a, b) = \mathrm{ggT}(|a|, |b|)$. □

Der Euklidische Algorithmus liefert aber noch etwas mehr als den größten gemeinsamen Teiler zweier Zahlen. Wir schauen uns das zunächst in einem Beispiel an.

Beispiel 1.1.13. Seien wieder $a = 17$ und $b = 3$ wie in Beispiel 1.1.10. Nach Satz 1.1.12 wissen wir nun dass $\mathrm{ggT}(a, b) = 1$. Wir schauen uns die Schritte des Euklidischen Algorithmus in diesem Beispiel noch einmal an:

$$17 = 5 \cdot 3 + 2 \tag{1.10}$$

$$3 = 1 \cdot 2 + 1 \tag{1.11}$$

$$2 = 2 \cdot 1 + 0. \tag{1.12}$$

Der ggT steht dabei in Zeile 1.11 als Rest. Wenn wir danach auflösen erhalten wir

$$1 = 3 - 1 \cdot 2. \tag{1.13}$$

Die 2 in dieser Zeile steht aber auch in Zeile 1.10 als Rest, und wir können dort auflösen

$$2 = 17 - 5 \cdot 3. \tag{1.14}$$

Das setzen wir schließlich in 1.13 ein und erhalten

$$1 = 3 - 1 \cdot 2 = 3 - 1 \cdot (17 - 5 \cdot 3) = 6 \cdot 3 - 1 \cdot 17.$$

Wir haben also den größten gemeinsamen Teiler von a und b ausgedrückt als

$$\mathrm{ggT}(a, b) = c \cdot a + d \cdot b,$$

mit $c, d \in \mathbb{Z}$.
Man sieht dass dieselbe Vorgehensweise immer funktioniert. In Beispiel 1.1.11 hätten wir die vorletzte Zeile nach 2 auflösen können, und danach die auftauchende 22 mit Hilfe der ersten Zeile ersetzen können. Das ergäbe

$$\mathrm{ggT}(118, 24) = 2 = 5 \cdot 24 - 1 \cdot 118.$$

Wir wollen diese Aussage nun noch einmal formal beweisen:

Satz 1.1.14. *Seien $a, b \in \mathbb{Z}$. Dann gibt es $c, d \in \mathbb{Z}$ mit*

$$\mathrm{ggT}(a, b) = c \cdot a + d \cdot b.$$

Beweis. Wir führen wieder eine Induktion über die Anzahl der Schritte im Euklidischen Algorithmus durch. Falls der Algorithmus nach dem ersten Schritt abbricht haben wir $\mathrm{ggT}(a, b) = b = 0 \cdot a + 1 \cdot b$.
Es breche der Algorithmus nun nach $N + 1$ Schritten ab. Wir schreiben

$$a = n \cdot b + r \tag{1.15}$$

mit $0 < r < b$ und setzen $a_2 = b, b_2 = r$. Nun bricht der Algorithmus für das Paar (a_2, b_2) nach N Schritten ab, und wir wissen nach Induktionsvoraussetzung (und dem Beweis von Satz 1.1.12)

$$\mathrm{ggT}(a, b) = \mathrm{ggT}(a_2, b_2) = c \cdot a_2 + d \cdot b_2 = c \cdot b + d \cdot r,$$

für gewisse $c, d \in \mathbb{Z}$. Wir lösen 1.15 nach r auf und setzen ein:

$$\mathrm{ggT}(a, b) = c \cdot b + d \cdot (a - n \cdot b) = d \cdot a + (c - d \cdot n) \cdot b.$$

Das ist die gewünschte Darstellung. □

Definition 1.1.15. Zwei ganze Zahlen $a \neq 0, b \neq 0$ heißen teilerfremd, wenn $\mathrm{ggT}(a, b) = 1$ gilt. Das bedeutet gerade, dass sie außer ± 1 keine gemeinsamen Teiler haben.

Lemma 1.1.16. *Seien $a, b \in \mathbb{Z}$ teilerfremd. Falls dann $a|bc$ gilt für ein $c \in \mathbb{Z}$, so folgt schon $a|c$.*

Beweis. Mit Satz 1.1.14 erhalten wir eine Gleichung

$$1 = n \cdot a + m \cdot b.$$

Wir multiplizieren mit c und erhalten

$$c = cna + mbc.$$

Da nach Voraussetzung a ein Teiler von bc ist, ist a also ein Teiler von c. □

1.1.4 Lineare diophantische Gleichungen

Ein ganzzahliges Polynom f in den Unbekannten $x_1, \ldots, x_n$ ist ein Ausdruck, den man aus ganzen Zahlen und den Unbekannten durch Addition und Multiplikation bilden kann. Beispiele sind etwa

$$f = 1 + x_1 x_2 - 3x_3^2$$

oder

$$f = -x_2 x_1^4 + 23x_5 + x_3 - x_7.$$

Eine *diophantische Gleichung* ist nun eine Gleichung der Gestalt

$$f(x_1, \ldots, x_n) = 0$$

wobei f ein ganzzahliges Polynom in den Unbekannten $x_1, \ldots, x_n$ ist. Ein Beispiel für eine diophantische Gleichung ist also

$$1 + x_1 x_2 - 3x_3^2 = 0.$$

Ein weiteres bekanntes Beispiel ist

$$x^2 + y^2 - z^2 = 0, \tag{1.16}$$

das die Unbekannten x, y, z benutzt und auch oft umgestellt wird zu

$$x^2 + y^2 = z^2.$$

Zu einer gegebenen diophantischen Gleichung interessiert man sich nun für *ganzzahlige* Lösungen, also für Tupel $a = (a_1, \ldots, a_n) \in \mathbb{Z}^n$ mit

$$f(a_1, \ldots, a_n) = 0.$$

Eine bekannte Lösung für 1.16 ist zum Beispiel das Tripel $(3, 4, 5)$.
Man möchte also im Allgemeinen herausfinden, ob eine diophantische Gleichung ganzzahlige Lösungen besitzt, wie man gegebenenfalls eine finden kann, und wie man besser noch *alle* ganzzahligen Lösungen bestimmen kann. Für beliebige diophantische Gleichungen kann das extrem schwer sein. So ist beispielsweise die Unlösbarkeit der Gleichung

$$x^n + y^n - z^n = 0 \tag{1.17}$$

für alle $n \geq 3$ der sogenannte *letzte Satz von Fermat*, der erst etwa 300 Jahre nach Fermat im Jahr 1994 durch Andrew Wiles bewiesen wurde. Hier soll noch einmal betont werden, dann man sich nur für *ganzzahlige* Lösungen interessiert. So hat 1.17 durchaus reelle Lösungen, wie etwa das Tripel $(1, 1, \sqrt[n]{2})$.
Einfacher zu lösen sind *lineare* diophantische Gleichungen. Dabei handelt es sich um Gleichungen der Gestalt

$$c_1x_1 + c_2x_2 + \cdots + c_nx_n - c = 0,$$

oder umgestellt

$$c_1x_1 + c_2x_2 + \cdots + c_nx_n = c.$$

Dabei sind wieder $c_1, \ldots, c_n, c \in \mathbb{Z}$ ganze Zahlen.

Beispiel 1.1.17. Gegeben sei die lineare diophantische Gleichung

$$3x_1 - 5x_2 = 8.$$

Wir sehen direkt, dass $(1, -1)$ eine ganzzahlige Lösung dieser Gleichung ist. Wenn nun (a_1, a_2) eine weitere Lösung ist, dann gilt

$$3(1 - a_1) - 5(-1 - a_2) = 3 + 5 - (3a_1 - 5a_2) = 8 - 8 = 0,$$

also ist $(1 - a_1, -1 - a_2)$ eine Lösung der *homogenen* linearen Gleichung $3x_1 - 5x_2 = 0$. Es ist aber relativ leicht, alle Lösungen (u_1, u_2) der homogenen Gleichung zu bestimmen. Es sind ja gerade die Tupel mit

$$3u_1 = 5u_2.$$

Mit Hilfe von Lemma 1.1.16 sehen wir, dass dies genau die Vielfachen des Tupels $(5, 3)$ sind. Insgesamt ist also

$$(1, -1) - (a_1, a_2) = (5t, 3t)$$

mit $t \in \mathbb{Z}$, und also ist

$$(a_1, a_2) = (1 - 5t, -1 - 3t), t \in \mathbb{Z}$$

eine gesamte Beschreibung der ganzzahligen Lösungsmenge.

Beispiel 1.1.18. Gegeben sei die lineare diophantische Gleichung

$$4x_1 + 10x_2 = 1.$$

Für jedes beliebige Tupel $(a_1, a_2) \in \mathbb{Z}^2$ ist die rechte Seite $4a_1 + 10a_2$ durch 2 teilbar. Die rechte Seite ist allerdings nicht durch 2 teilbar. Also besitzt die Gleichung keine ganzzahlige Lösung.

In Beispiel 1.1.17 haben wir die Gesamtheit aller Lösungen durch eine *Partikularlösung* der Gleichung und die Lösungsmenge der *homogenen* Gleichung erhalten. Diese Vorgehensweise ist aus der linearen Algebra zur Lösung linearer Gleichungssysteme bekannt, und funktioniert auch hier:

Lemma 1.1.19. *Gegeben sei die lineare diophantische Gleichung*

$$c_1x_1 + \cdots + c_nx_n = c. \tag{1.18}$$

Sei $a = (a_1, \ldots, a_n) \in \mathbb{Z}^n$ eine beliebige Lösung der Gleichung, und sei

$$L' = \{(b_1, \ldots, b_n) \in \mathbb{Z}^n \mid c_1b_1 + \cdots + c_nb_n = 0\}$$

die Lösungsmenge der homogenen Gleichung. Dann erhält man die Gesamtmenge aller Lösungen der Gleichung 1.18 als

$$L = a + L' = \{a + b \mid b \in L'\}.$$

Beweis. Für $b = (b_1, \ldots, b_n) \in L'$ ist $a + b = (a_1 + b_1, \ldots, a_n + b_n)$. Es gilt nun

$$\begin{aligned} c_1(a_1 + b_1) + \cdots + c_n(a_n + b_n) &= c_1a_1 + \cdots + c_na_n + c_1b_1 + \cdots + c_nb_n \\ &= c + 0 \\ &= c. \end{aligned}$$

Also ist $a + b$ eine Lösung von 1.18. Sei umgekehrt $u = (u_1, \ldots, u_n) \in \mathbb{Z}^n$ eine Lösung von 1.18. Dann ist $u - a$ eine Lösung der homogenen Gleichung, wie man analog zu eben sofort nachrechnet. Also ist $b := u - a \in L'$, und $u = a + b$. □

Wir beschränken uns nun auf den Fall $n = 2$.

Satz 1.1.20. *Gegeben sei die diophantische Gleichung*

$$c_1 x_1 + c_2 x_2 = c.$$

(i) Die Gleichung ist genau dann lösbar, wenn $\mathrm{ggT}(c_1, c_2) | c$, *also*

$$c = r \cdot \mathrm{ggT}(c_1, c_2)$$

für ein $r \in \mathbb{Z}$. *Ist in diesem Falle* $\mathrm{ggT}(c_1, c_2) = a_1 c_1 + a_2 c_2$ *mit* $a_1, a_2 \in \mathbb{Z}$, *so ist*

$$(ra_1, ra_2)$$

eine Lösung der Gleichung.

(ii) Ist $c_1 = \tilde{c}_1 \cdot \mathrm{ggT}(c_1, c_2)$ *und* $c_2 = \tilde{c}_2 \cdot \mathrm{ggT}(c_1, c_2)$, *so sind die Lösungen der homogenen Gleichung gerade die Tupel*

$$(t \cdot \tilde{c}_2, -t \cdot \tilde{c}_1) \quad \textit{mit } t \in \mathbb{Z}.$$

Beweis. Setze $d := \mathrm{ggT}(c_1, c_2)$. Nach Satz 1.1.14 gibt es eine Gleichung

$$d = a_1 c_1 + a_2 c_2$$

mit $a_1, a_2 \in \mathbb{Z}$.
(i) Wenn die Gleichung eine Lösung (u_1, u_2) besitzt, so teilt d offensichtlich $c_1 u_1 + c_2 u_2 = c$. Sei umgekehrt $c = r \cdot d$. Dann ist

$$c = r(a_1 c_1 + a_2 c_2) = c_1 r a_1 + c_2 r a_2.$$

Also ist (ra_1, ra_2) eine Lösung.
(ii) Zunächst ist jedes $(t\tilde{c}_2, -t\tilde{c}_1)$ eine Lösung der homogenen Gleichung, denn

$$c_1 t\tilde{c}_2 - c_2 t\tilde{c}_1 = t(c_1\tilde{c}_2 - c_2\tilde{c}_1) = t(d\tilde{c}_1\tilde{c}_2 - d\tilde{c}_2\tilde{c}_1) = 0.$$

Sei nun (b_1, b_2) eine beliebige Lösung der homogenen Gleichung, d.h. $c_1 b_1 = -c_2 b_2$. Nach Kürzen von d auf beiden Seiten bleibt

$$\tilde{c}_1 b_1 = -\tilde{c}_2 b_2, \tag{1.19}$$

und $\mathrm{ggT}(\tilde{c}_1, \tilde{c}_2) = 1$. Aus Lemma 1.1.16 folgt $\tilde{c}_1 | b_2$ und $\tilde{c}_2 | b_1$. Schreiben wir also $b_1 = t_1\tilde{c}_2, b_2 = t_2\tilde{c}_1$, so folgt aus 1.19 $t_1 = -t_2$. Das ist genau die Behauptung. □

Insgesamt haben wir damit eine Methode, lineare diophantische Gleichungen in zwei Variablen komplett zu lösen. Wir verwenden Satz 1.1.20 und Lemma 1.1.19, zusammen mit dem Euklidischen Algorithmus.

Beispiel 1.1.21. Wir betrachten die diophantische Gleichung

$$17x_1 + 3x_2 = 44.$$

Aus Beispiel 1.1.10 wissen wir

$$\mathrm{ggT}(17, 3) = 1,$$

und 1 ist offensichtlich Teiler von 44. Damit ist die Gleichung lösbar. Aus Beispiel 1.1.13 wissen wir nun

$$1 = -1 \cdot 17 + 6 \cdot 3.$$

Also ist $(-44, 6 \cdot 44) = (-44, 264)$ eine Lösung. Aus Teil (ii) in Satz 1.1.20 sehen wir dass die Lösungen der homogenen Gleichung gerade von der Gestalt

$$(3t, -17t)$$

mit $t \in \mathbb{Z}$ sind. Lemma 1.1.19 liefert uns damit die gesamte ganzzahlige Lösungsmenge

$$L = \{(3t - 44, 264 - 17t) \mid t \in \mathbb{Z}\}.$$

Beispiel 1.1.22. Wir betrachten

$$118x_1 + 24x_2 = 9.$$

Aus Beispiel 1.1.11 wissen wir $\mathrm{ggT}(118, 24) = 2$, und das ist kein Teiler von 9. Also besitzt die Gleichung keine ganzzahligen Lösungen.

Bemerkung 1.1.23. Man kann Satz 1.1.20 auch auf lineare diophantische Gleichungen in mehr als zwei Variablen verallgemeinern. Bei einer Gleichung

$$c_1x_1 + \cdots + c_nx_n = c$$

ist die Lösbarkeitsbedingung beispielsweise gerade

$$\mathrm{ggT}(c_1, \ldots, c_n) | c.$$

Die Lösungen kann man dann induktiv über die Anzahl der Variablen erhalten. Wir wollen das hier aber nicht im Detail ausführen.

1.1.5 Primzahlen

Wir wollen uns in diesem Kapitel mit Primzahlen beschäftigen. Die bekannteste Definition ist die folgende:

Definition 1.1.24. Eine Zahl $p \in \mathbb{Z} \setminus \{1, -1\}$ heißt Primzahl, wenn sie außer ± 1 und $\pm p$ keine weiteren Teiler hat.

Bemerkung 1.1.25. (1) Die Null ist keine Primzahl. Es gilt zum Beispiel $0 = 0 \cdot 7$, also ist 7 ein Teiler von 0.
(2) Die 1 und die -1 sind keine Primzahlen, und zwar per Definition. Die Teilerbedingung würden sie nämlich erfüllen.
(3) p ist genau dann prim wenn $-p$ prim ist. Wir können uns deshalb auf die Untersuchung positiver Primzahlen beschränken.

Beispiel 1.1.26. Die Liste der positiven Primzahlen beginnt bekannterweise wie folgt:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, \ldots$$

Die größte bekannte Primzahl ist derzeit $p = 2^{43112609} - 1$.

Der folgende Satz liefert eine äquivalente Beschreibung von Primzahlen:

Satz 1.1.27. *Eine Zahl $p \in \mathbb{Z} \setminus \{1, -1\}$ ist genau dann prim, wenn für alle $a, b \in \mathbb{Z}$ aus $p|ab$ immer schon $p|a$ oder $p|b$ folgt.*

Beweis. Sei p prim, und es gelte $p|ab$. Wir können annehmen dass p nicht a teilt, sonst wären wir ja bereits fertig. Also muss $\mathrm{ggT}(a, p) = 1$ sein, da p ja außer $\pm 1, \pm p$ keine weiteren Teiler hat. Aus Lemma 1.1.16 folgt also $p|b$.
Erfülle nun umgekehrt p die Produktbedingung. Wir zeigen dass p prim ist. Sei also $p = ab$. Da offensichtlich $p|p$ gilt, folgt ohne Beschränkung der Allgemeinheit $p|a$ aus der Produktbedingung. Also gilt $a = r \cdot p$ und wir erhalten insgesamt

$$p = prb.$$

Da $p \neq 0$ geht das aber nur wenn $rb = 1$, also $b = \pm 1$ ist. Daraus folgt schließlich $a = \pm p$. Also hat p außer $\pm 1, \pm p$ keine weiteren Teiler und ist somit prim im Sinne der ursprünglichen Definition. □

Oft wird die Produktbedingung, also dass p ein Produkt nur dann teilt wenn es einen der Faktoren teilt, als eigentliche Definition von Primzahl verwendet. Unsere ursprüngliche Definition, dass p keine nichttrivialen Teiler hat, wird dagegen oft als *Irreduzibilität* bezeichnet. Wir haben gesehen, dass beide Definition für ganze Zahlen übereinstimmen.

Wir wollen nun die bekannte Aussage über die Primfaktorzerlegung ganzer Zahlen beweisen:

Satz 1.1.28. *Jede ganze Zahl $a \neq 0$ lässt sich als ein Produkt*

$$a = v \cdot p_1 \cdot p_2 \cdots p_n$$

schreiben, wobei $v = \pm 1$ und alle p_i positive Primzahlen sind. Die p_i sind dabei bis auf Reihenfolge eindeutig bestimmt.

Beweis. Wir können uns offensichtlich auf positive Zahlen $a > 0$ beschränken. Wir beweisen zunächst die Existenz der Zerlegung, und zwar per Induktion. Der Induktionsanfang ist $a = 1$, mit der Zerlegung $a = 1$, in der gar keine Primzahlen auftreten.
Wir nehmen nun an, dass jede Zahl $\leq N$ eine Primfaktorzerlegung besitzt. Nun betrachten wir $a = N + 1$. Falls a selbst prim ist hat es die Zerlegung $a = a$. Falls nicht, können wir $a = bc$ schreiben mit $0 < b, c < a$. Nach Induktionsvoraussetzung besitzen nun b und c Primfaktorzerlegungen, und durch multiplizieren dieser Zerlegungen entsteht eine solche für a.
Nun müssen wir die Eindeutigkeit der Primfaktorzerlegung beweisen. Wir nehmen dazu an, dass eine positive ganze Zahl existiert, die zwei verschiedene Primfaktorzerlegungen besitzt. Sei dabei a als die kleinste aller solcher Zahlen angenommen. Dann kann in zwei verschiedenen Zerlegungen kein gemeinsamer Primfaktor auftauchen, weil sonst nach Kürzung dieses Faktors eine kleinere Zahl schon zwei verschiedene Zerlegungen hätte. Wir nehmen nun zwei verschiedene Zerlegungen und isolieren dabei verschiedene Primzahlen:

$$a = p \cdot b = q \cdot c \tag{1.20}$$

mit $p \neq q$ beide prim. Mit Lemma 1.1.16 (oder Satz 1.1.27) folgt aus $p|qc$ nun also $p|c$. Wegen $c < a$ ist die Primfaktorzerlegung von c aber eindeutig, und also kam p darin vor. Damit kam der Faktor p aber doch in beiden Zerlegungen von a vor, ein Widerspruch. □

Der folgende berühmte Satz geht bis auf Euklid zurück:

Satz 1.1.29. *Es gibt unendlich viele Primzahlen.*

Beweis. Sei $p_1, \ldots, p_n$ die Liste der ersten n positiven Primzahlen. Setze

$$a = (p_1 \cdots p_n) + 1.$$

Nach Satz 1.1.28 hat a mindestens einen positiven Primfaktor. Das kann aber keiner der $p_1, \ldots, p_n$ sein, da er sonst mit a und $p_1 \ldots p_n$ auch 1 teilen würde. Also muss es eine weitere (und also größere) Primzahl geben. □

Besonders interessant ist die Verteilung der Primzahlen innerhalb der ganzen Zahlen. Man kann relativ einfach beweisen, dass es beliebig lange Intervalle gibt, in denen keine Primzahl auftaucht. Sei dazu $n \geq 2$ eine ganze Zahl und

$$n! = n \cdot (n-1) \cdots 2 \cdot 1$$

ihre sogenannte *Fakultät*. Man sieht nun dass für $2 \leq j \leq n$ keine der Zahlen

$$n! + j$$

eine Primzahl sein kann. In der Tat ist ja j ein Teiler beider Summanden, und also ein Teiler der Summe. Gleichzeitig ist die Summe aber echt größer als j. Also haben wir $n-1$ aufeinanderfolgende Zahlen konstruiert, von denen keine eine Primzahl ist:

Satz 1.1.30. *Es gibt beliebig lange Intervalle in $\mathbb{Z}$, die keine Primzahl enthalten.*

Ein anderer Satz besagt wiederum, in welchen Intervallen man immer eine Primzahl finden kann. Der Beweis ist elementar, aber zu aufwändig für diese Vorlesung. Wir zitieren das Resultat deshalb nur:

Satz 1.1.31. *Für jede ganze Zahl $n \geq 1$ gibt es eine Primzahl p mit*

$$n < p \leq 2n.$$

1.1.6 Die Euler'sche φ-Funktion

In diesem Abschnitt wollen wir die Euler'sche φ-Funktion einführen, und einige ihrer Eigenschaften untersuchen. Sie wird im nächsten Kapitel, und auch später für die Kryptographie noch von Bedeutung sein.
Für eine positive ganze Zahl $n \geq 1$ definieren wir $\varphi(n)$ als die Anzahl aller Zahlen $1 \leq k \leq n$, die teilerfremd zu n sind. Also

$$\varphi(n) = \#\{k \mid 1 \leq k \leq n, \mathrm{ggT}(k,n) = 1\}.$$

Beispiel 1.1.32. Die ersten Werte sind

$$\varphi(1) = 1,\ \varphi(2) = 1,\ \varphi(3) = 2,\ \varphi(4) = 2,\ \varphi(5) = 4,\ \varphi(6) = 2, \ldots$$

Der Verlauf der Werte scheint also nicht direkt vorhersehbar zu sein. Um den Wert der Euler'schen φ-Funktion dennoch für beliebige Zahlen ausrechnen zu können, beweisen wir den folgenden Satz. Er erlaubt uns die Berechnung von $\varphi(n)$, vorausgesetzt wir kennen eine Zerlegung von n in Primfaktoren:

Satz 1.1.33. *Sei p eine Primzahl und r, n, m positive ganze Zahlen. Dann gilt:*

(i) $\varphi(p) = p - 1$.

(ii) $\varphi(p^r) = p^{r-1}(p-1) = p^r - p^{r-1}$.

(iii) Falls m und n teilerfremd sind ist $\varphi(mn) = \varphi(m)\varphi(n)$.

Beweis. (i) Offensichtlich ist jede Zahl $1 \leq k < p$ teilerfremd zu p, wenn p prim ist. Daraus folgt $\varphi(p) = p - 1$. Außerdem ist (i) ein Spezialfall von:
(ii) Eine Zahl k ist genau dann *nicht* teilerfremd zu p^r, wenn $p|k$. Die positiven Zahlen die von p geteilt werden sind aber gerade

$$p, 2p, 3p, \ldots$$

Kleiner gleich p^r sind davon gerade p^{r-1} viele. Also müssen wir p^{r-1} Zahlen zwischen 1 und p^r entfernen, um $\varphi(p^r)$ zu berechnen. Dann bleiben aber gerade

$$p^r - p^{r-1} = p^{r-1}(p-1)$$

viele übrig.
Teil (iii) werden wir im zweiten Teil der Vorlesung beweisen (Satz 2.2.25) . Mit etwas mehr Theorie wird es sehr einfach sein. □

Beispiel 1.1.34. Wir berechnen $\varphi(100)$. Dazu finden wir die Primfaktorzerlegung

$$100 = 2^2 \cdot 5^2$$

und rechnen

$$\varphi(100) = \varphi(2^2) \cdot \varphi(5^2) = 2 \cdot 1 \cdot 5 \cdot 4 = 40.$$

Es gibt also 40 Zahlen kleiner als 100, die teilerfremd zu 100 sind.

Beispiel 1.1.35. Wir finden

$$\varphi(12) = \varphi(3 \cdot 4) = \varphi(3) \cdot \varphi(4) = 2 \cdot 2 = 4.$$

Es gibt also 4 Zahlen kleiner als 12 die teilerfremd zu 12 sind. Das sind gerade

$$1, 5, 7, 11.$$

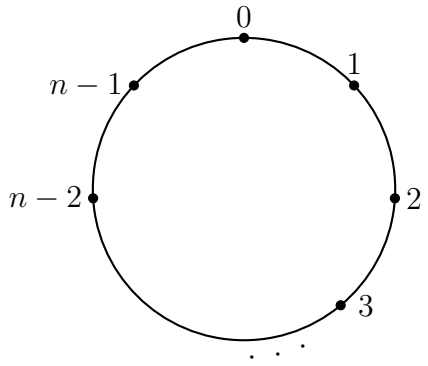
1.2 Die Restklassenringe $\mathbb{Z}/n\mathbb{Z}$

Die Mathematik als Fachgebiet ist so ernst, daß man keine Gelegenheit versäumen sollte, dieses Fachgebiet unterhaltsamer zu gestalten.

Blaise Pascal (1623-1662)

1.2.1 Konstruktion

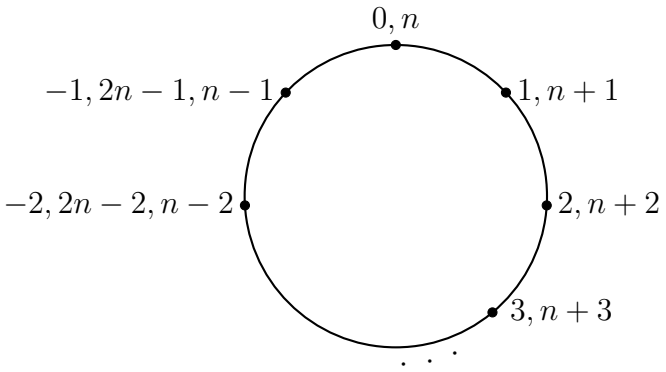
Das Rechnen in den sogenannten *Restklassenringen von* $\mathbb{Z}$ ist uns interessanterweise absolut vertraut, ohne dass wir das gewöhnlich wissen. Fragt uns jemand um 23 Uhr, wieviel Uhr es in 4 Stunden sein wird, rechnet keiner von uns 23+4=27 und gibt „27 Uhr" zur Antwort. Sondern wir setzen ganz selbstverständlich 24=0 und zählen von 0 aus weiter. Deshalb ist die Antwort gewöhnlich „3 Uhr". Wir stellen uns nun eine Uhr vor, die in n Stunden eingeteilt ist:



Wenn wir Zahlen zwischen 0 und $n-1$ addieren wollen, addieren wir sie genau wie gewöhnlich die Uhrzeit. Es ist z.B.

$$(n-2)+3=1$$

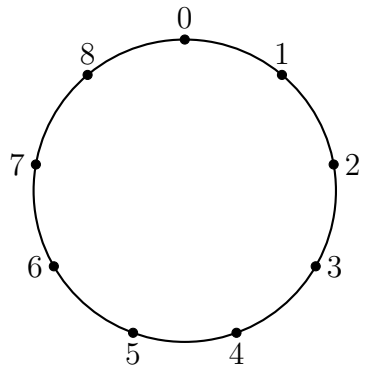
Wir können auch die Uhr noch mit größeren und kleineren ganzen Zahlen beschriften, in dem wir im Uhrzeigersinn bzw gegen den Uhrzeigersinn einfach weitermachen:



Jetzt können wir nämlich die Addition auch wie gewohnt durchführen, und dann als Ergebnis aber die kleinste der beieinanderstehenden Zahlen ausgeben. Also $(n-2)+3$ ergibt eigentlich $n+1$, aber $n+1$ ist das selbe wie 1, also geben wir 1 als Ergebnis aus. So können wir nun auch die Multiplikation ausführen. Wir rechen zum Beispiel $2 \cdot (n-1) = 2n-2$, und geben aber $n-2$ als Ergebnis aus.

Wir sehen, dass wir eigentlich wie in $\mathbb{Z}$ rechnen, nur dass gewisse Zahlen miteinander identifiziert werden.

Zur Veranschaulichung rechnen wir ein paar explizite Beispiele für $n = 9$:



Es gilt zum Beispiel

$$1+2=3 \qquad 3+6=0 \qquad 7+8=6$$

und

$$2 \cdot 3 = 6 \qquad 3 \cdot 3 = 0 \qquad 4 \cdot 5 = 2.$$

Das ganze wollen wir nun etwas formaler definieren. Sei dazu stets eine positive ganze Zahl $n \geq 2$ fixiert. Wir definieren nun eine Äquivalenzrelation $\equiv_n$ auf $\mathbb{Z}$ wie folgt:

$$a \equiv_n b \quad :\Longleftrightarrow \quad n|(a-b).$$

Wir sagen auch a *ist kongruent* b *modulo* n, falls $a \equiv_n b$. Manchmal schreiben wir dafür auch

$$a \equiv b \bmod n.$$

Zwei Zahlen sind also kongruent modulo n, falls ihre Differenz durch n teilbar ist. Das bedeutet gerade, dass sie bei Teilung durch n den selben Rest lassen. Im Bild der Uhr sind zwei Zahlen genau dann kongruent, wenn sie an der selben Stelle auf der Uhr stehen. Modulo 9 gilt also zum Beispiel

$$9 \equiv_9 0 \text{ und } 4 \equiv_9 13.$$

Lemma 1.2.1. $\equiv_n$ *ist eine Äquivalenzrelation auf* $\mathbb{Z}$.

Beweis. Es ist zunächst die Reflexivität zu zeigen, also $a \equiv_n a$ für alle $a \in \mathbb{Z}$. Das ist aber klar, da

$$a - a = 0,$$

und 0 von n geteilt wird, da $0 = 0 \cdot n$.
Für die Symmetrie gelte $a \equiv_n b$, also $r \cdot n = a - b$. Dann gilt aber

$$b - a = (-r) \cdot n,$$

also teilt n auch $b - a$, und also ist $b \equiv_n a$.
Um die Transitivität zu zeigen setzen wir $a \equiv_n b$ und $b \equiv_n c$ voraus. Wir müssen $a \equiv_n c$ zeigen. Nach Definition gilt

$$r \cdot n = a - b \text{ und } s \cdot n = b - c.$$

Daraus folgt

$$(r+s) \cdot n = r \cdot n + s \cdot n = (a-b) + (b-c) = a - c.$$

Also teilt n auch $a - c$, und das bedeutet $a \equiv_n c$. □

Wir können nun die Äquivalenzklassen der Äquivalenzrelation betrachten. Eine Äquivalentklasse ist dabei gerade die Menge aller Elemente, die zueinander in

der Relation stehen. Für jedes $a \in \mathbb{Z}$ bezeichnen wir die Äquivalenzklasse von a mit $[a]_n$. Es ist also

$$[a]_n = \{b \in \mathbb{Z} \mid a \equiv_n b\} = \{b \in \mathbb{Z} \mid n|(a-b)\} = \{a + k \cdot n \mid k \in \mathbb{Z}\}\,.$$

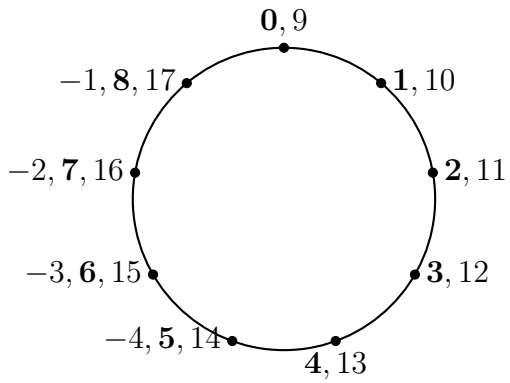
Man nennt die Äquivalenzklassen dann auch *Restklassen modulo* n. Eine Restklassse ist also die Menge aller Zahlen, in auf der Uhr an der selben Stelle stehen:

$$[8]_9 = \{\ldots, -1, 8, 17 \ldots\}$$

Äquivalente Zahlen ergeben dieselbe Restklasse, zum Beispiel ist

$$[3]_9 = [12]_9.$$

In jeder der Restklassen liegt genau eine der Zahlen zwischen 0 und $n-1$. Die Zahlen 0 bis $n-1$ nennt man deshalb auch ein *vollständiges Vertretersystem* der Restklassen. Dieser kanonische Vertreter einer Zahl ist genau ihr Rest bei Division durch n.



Die Menge der Restklassen von $\mathbb{Z}$ bezüglich der Äquivalenzrelation $\equiv_n$ wird mit $\mathbb{Z}/n\mathbb{Z}$ bezeichnet. Es ist also

$$\mathbb{Z}/n\mathbb{Z} = \{[a]_n \mid a \in \mathbb{Z}\} = \{[0]_n, [1]_n, \ldots, [n-1]_n\}\,.$$

Wir definieren nun Addition und Multiplikation auf Restklassen:

$$[a]_n + [b]_n = [a+b]_n$$

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

Die Verknüpfungen sind also einfach *vertreterweise* definiert: Wir entnehmen jeder der beiden Restklassen einen Vertreter, verknüfpen die Vertreter wie gewohnt in $\mathbb{Z}$, und bilden dann wieder die Restklasse. Im Bild der Uhr bedeutet das, dass wir aus jeder der gewünschten Positionen eine der dort stehenden Zahlen nehmen, diese Zahlen addieren oder multiplizieren, und als Ergebnis die Position ausgeben, an der das Ergebnis steht. So bekommen wir zum Beispiel

$$[1]_9 + [3]_9 = [1 + 3]_9 = [4]_9.$$

Hier könnte es nun ein Problem geben. Sie Restklasse $[1]_9$ ist ja mit der Restklasse $[10]_9$ identisch. Wir hätten also genauso rechnen können

$$[1]_9 + [3]_9 = [10]_9 + [3]_9 = [13]_9.$$

Erfreulicherweise sehen wir auf der Uhr, dass 4 und 13 an der selben Stelle stehen, also $[4]_9 = [13]_9$ gilt. Beide Rechnungen ergeben also das selbe Ergebnis. Wir beweisen nun, dass sich das immer so verhält. Der Einfachheit halber lassen wir ab sofort den unteren Index n bei den Restklassen für gewöhnlich weg.

Lemma 1.2.2. *Die Verknüpfungen $+$ und $\cdot$ sind auf $\mathbb{Z}/n\mathbb{Z}$ ist wohldefiniert, d.h. unabhängig von der Wahl der Vertreter.*

Beweis. Seien $a, a', b, b' \in \mathbb{Z}$ mit $[a] = [a']$ und $[b] = [b']$. Wir müssen zeigen dass

$$[a + b] = [a' + b'] \text{ und } [a \cdot b] = [a' \cdot b']$$

gilt. Nach Annahme gilt $a \equiv a'$, also $r \cdot n = a - a'$, und analog $s \cdot n = b - b'$, für gewissen $r, s \in \mathbb{Z}$. Daraus folgt

$$(r + s) \cdot n = a - a' + b - b' = (a + b) - (a' + b')$$

Daraus folgt $(a + b) \equiv (a' + b')$, und also $[a + b] = [a' + b']$, die erste erwünschte Aussage.
Für die zweite verwenden wir

$$rnb = (a - a')b = ab - a'b$$

und

$$a'sn = a'(b - b') = a'b - a'b'.$$

Wenn wir linke und rechte Seite jeweils addieren, bekommen wir

$$brn + a'sn = ab - a'b'.$$

Wenn wir n links ausklammern sehen wir, dass n ein Teiler von $ab - a'b'$ ist. Also erzeugen ab und $a'b'$ dieselbe Restklasse. Das ist die zweite erwünschte Aussage. □

Satz 1.2.3. *Für die Addition und Multiplikation in $\mathbb{Z}/n\mathbb{Z}$ gelten die Regeln (1.1)-(1.8) wie in $\mathbb{Z}$. Das neutrale Element bezüglich $+$ ist $[0]$, das neutrale Element bezüglich $\cdot$ ist $[1]$. Das inverse Element zu $[a]$ bezüglich $+$ ist $[-a]$.*

Beweis. Nachdem wir die Wohldefiniertheit der vertreterweise definierten Verknüpfungen gezeigt haben, ist die Aussage klar. Es gilt ja zum Beispiel

$$[a] + [b] = [a + b] = [b + a] = [b] + [a],$$

wobei wir das Kommutativgesetz in $\mathbb{Z}$ verwendet haben. Ebenso gilt etwa

$$[0] + [a] = [0 + a] = [a].$$

Der Rest geht analog. □

Definition 1.2.4. Wir nennen die Menge $\mathbb{Z}/n\mathbb{Z}$ mit $+$ und $\cdot$ den *Restklassenring modulo n von $\mathbb{Z}$.*

Beispiel 1.2.5. Wir führen nochmals einige Rechnungen in $\mathbb{Z}/9\mathbb{Z}$ vor:

$$-[3] = [-3] = [6] \qquad -[1] = [-1] = [8]$$

$$[6] + [3] = [9] = [0] \qquad [1] + [8] = [9] = [0]$$

$$[3] \cdot [3] = [9] = [0]$$

$$[3] \cdot [1] = [3] = [21] = [3] \cdot [7], \qquad [1] \neq [7]$$

$$[4] \cdot [7] = [4 \cdot 7] = [28] = [1]$$

In den letzten Zeilen sehen wir, dass $\mathbb{Z}/n\mathbb{Z}$ Eigenschaften hat, die es von $\mathbb{Z}$ stark unterscheidet. So kann das Produkt von zwei Elementen Null sein, obwohl keines der Elemente Null war. Auch die Kürzungsregel gilt im Allgemeinen nicht. Hingegen kann man zum Beispiel die Restklasse $[4]$ multiplikativ invertieren. In $\mathbb{Z}$ gibt es keine Zahl a mit $4 \cdot a = 1$. Anders gesagt hat die Gleichung

$$4x = 1$$

keine Lösung in $\mathbb{Z}$, aber eine in $\mathbb{Z}/9\mathbb{Z}$, nämlich $x = [7]$. Das wollen wir im nächsten Abschnitt genauer untersuchen.

1.2.2 Eigenschaften

Für gegebene $[a], [b] \in \mathbb{Z}/n\mathbb{Z}$ möchten wir gerne die Gleichung

$$[a] \cdot [x] = [b] \tag{1.21}$$

in $\mathbb{Z}/n\mathbb{Z}$ lösen.

Satz 1.2.6. *Die Gleichung $[a] \cdot [x] = [b]$ besitzt genau dann eine Lösung $[x] \in \mathbb{Z}/n\mathbb{Z}$, wenn*

$$\mathrm{ggT}(a, n) | b$$

gilt. Es gibt dann genau $\mathrm{ggT}(a, n)$ viele Lösungen in $\mathbb{Z}/n\mathbb{Z}$.

Beweis. Im Prinzip haben wir das schon bei den diophantischen Gleichungen bewiesen. Die Gleichung ist ja äquivalent zu $0 = [ax - b]$, d.h. wir suchen ein x, so dass $ax - b$ ein Vielfaches von n ist. Wir suchen also ganze Zahlen x *und* y mit

$$ax + ny = b. \tag{1.22}$$

Die Lösbarkeitsbedingung für diese diophantische Gleichung ist aber gerade $\mathrm{ggT}(a, n) | b$, siehe Satz 1.1.20.
Jede weitere Lösung (x', y') von 1.22 ist aber von der Gestalt

$$(x', y') = (x, y) + t \cdot \left(\frac{n}{\mathrm{ggT}(a, n)}, -\frac{a}{\mathrm{ggT}(a, n)} \right),$$

mit $t \in \mathbb{Z}$. Also durchläuft

$$x + t \cdot \frac{n}{\mathrm{ggT}(a, n)}$$

alle Lösungen der ursprünglichen Gleichung. Zwei Zahlen ergeben aber genau dann dieselbe Restklasse in $\mathbb{Z}/n\mathbb{Z}$, wenn sie sich um ein Vielflaches von n unterscheiden. Damit sind die Restklassen

$$\left[x + t \cdot \frac{n}{\mathrm{ggT}(a, n)} \right]$$

mit $t = 0, \ldots, \mathrm{ggT}(a, n) - 1$ genau die verschiedenen Lösungen der ursprünglichen Gleichung. Es gibt also $\mathrm{ggT}(a, n)$ viele. □

Bemerkung 1.2.7. Wir sehen also auch, wie man die Gleichung $[a] \cdot [x] = [b]$ in $\mathbb{Z}/n\mathbb{Z}$ explizit löst. Wir müssen nur die diophantische Gleichung

$$ax + ny = b$$

in $\mathbb{Z}$ lösen. Die Restklassen der $[x]$ sind dann die gewünschten Lösungen. Wie man diophantische Gleichungen löst, haben wir in Abschnitt 1.1.4 gesehen.

Beispiel 1.2.8. In $\mathbb{Z}/10\mathbb{Z}$ suchen wir alle Lösungen der Gleichung

$$[4] \cdot [x] = [6].$$

Wegen $\mathrm{ggT}(4, 10) = 2$ und $2|6$ ist die Lösbarkeit sichergestellt. Wir suchen nun die Lösungen zu

$$4x + 10y = 6$$

in $\mathbb{Z}$. Wegen

$$2 = (-2) \cdot 4 + 1 \cdot 10$$

gilt

$$6 = (-6) \cdot 4 + 3 \cdot 10,$$

also ist $(x, y) = (-6, 3)$ eine spezielle Lösung. Alle Lösungen erhält man also als $(-6, 3) + t \cdot (5, -2)$, mit $t \in \mathbb{Z}$. Die x-Komponente ist dabei $-6 + 5t$, also

$$\ldots, -6, -1, 4, 9, \ldots$$

Da wir uns nur für die Restklassen in $\mathbb{Z}/10\mathbb{Z}$ interessieren, erhalten wir

$$[4] \text{ und } [9]$$

als Lösungen. Das sind genau $2 = \mathrm{ggT}(4, 10)$ viele.

Beispiel 1.2.9. Wir wollen in $\mathbb{Z}/5\mathbb{Z}$ die Gleichung

$$[3] \cdot [x] = [4]$$

lösen. Wegen $\mathrm{ggT}(3, 5) = 1$ ist die Gleichung lösbar, und es gibt genau eine Lösung. Es gilt

$$2 \cdot 3 - 1 \cdot 5 = 1,$$

und also

$$8 \cdot 3 - 4 \cdot 5 = 4.$$

In $\mathbb{Z}/5\mathbb{Z}$ erhalten wir also die Lösung

$$[8] = [3].$$

Beispiel 1.2.10. In $\mathbb{Z}/8\mathbb{Z}$ betrachten wir

$$[2] \cdot [x] = [5].$$

Weil $\mathrm{ggT}(2, 8) = 2$ kein Teiler von 5 ist, ist die Gleichung unlösbar.

Ein ganz spezieller Fall der betrachteten Gleichungen ist

$$[a] \cdot [x] = [1].$$

Hier fragen wir uns also gerade, ob die Restklasse $[a]$ in $\mathbb{Z}/n\mathbb{Z}$ *multiplikativ invertierbar* ist. Während das in $\mathbb{Z}$ für ganze Zahlen fast nie der Fall ist, haben wir in den Restklassenringen folgendes Ergebnis:

Korollar 1.2.11. *Ein Element $[a] \in \mathbb{Z}/n\mathbb{Z}$ ist multiplikativ invertierbar, genau dann wenn $\mathrm{ggT}(a, n) = 1$. Das multiplikativ inverse Element ist dann eindeutig bestimmt.*

Beweis. Spezialfall von Satz 1.2.6, mit $b = 1$. □

Korollar 1.2.12. *Es gibt genau $\varphi(n)$ invertierbare Elemente in $\mathbb{Z}/n\mathbb{Z}$, wobei φ die Euler'sche φ-Funktion ist.*

Satz 1.2.13. *Ist p eine Primzahl, so sind alle Elemente $0 \neq [a]$ in $\mathbb{Z}/p\mathbb{Z}$ multiplikativ invertierbar.*

Beweis. Für alle $a \in \{1, \ldots, p-1\}$ gilt $\mathrm{ggT}(a, p) = 1$. □

Beispiel 1.2.14. Wir suchen alle multiplikativ invertierbaren Element in $\mathbb{Z}/8\mathbb{Z}$. Wir suchen also alle Zahlen $1 \leq k < 8$, die teilerfremd zu 8 sind. Das sind $1, 3, 5, 7$, also die Restklassen

$$[1], [3], [5], [7].$$

Wollen wir zum Beispiel das inverse zu $[3]$ finden, müssen wir wie oben die Gleichung $[3] \cdot [x] = [1]$ lösen. Wie üblich finden wir die folgende Gleichung, notfalls mit dem euklidischen Algorithmus:

$$1 = 3 \cdot 3 - 1 \cdot 8.$$

Der Übergang zu Restklassen liefert

$$[1] = [3] \cdot [3].$$

Also ist $[3]$ hier sein eigenes multiplikativ Inverses.

Beispiel 1.2.15. In $\mathbb{Z}/17\mathbb{Z}$ ist jedes Element $0 \neq [a]$ multiplikativ invertierbar. Um beispielsweise $[9]$ zu invertieren lösen wir wieder

$$9x + 17y = 1 :$$

$$2 \cdot 9 - 1 \cdot 17 = 1.$$

Also ist $[2]$ das Inverse zu $[9]$.

Bemerkung 1.2.16. Falls $[a]$ multiplikativ invertierbar ist, lassen sich die Gleichungen

$$[a] \cdot [x] = [b]$$

natürlich besonders einfach lösen. Man multipliziert einfach beide Seiten mit dem Inversen von $[a]$. Beispielsweise erhält man in $\mathbb{Z}/17\mathbb{Z}$ eine Lösung für

$$[9] \cdot [x] = [3]$$

durch

$$[x] = [2] \cdot [3] = [6].$$

1.2.3 Bekannte Teilbarkeitsregeln

Eine aus der Schule bekannte Regel ist die folgende:

Satz 1.2.17. *Eine ganze Zahl ist genau dann durch 3 teilbar, wenn ihre Quersumme durch 3 teilbar ist.*

Nachdem wir die Restklassenringe von $\mathbb{Z}$ eingeführt haben, lässt sich diese und andere Regeln sehr einfach beweisen. Dazu bemerken wir zuerst noch einmal, dass eine Zahl $a \in \mathbb{Z}$ genau dann durch 3 teilbar ist, wenn $[a] = [0]$ in $\mathbb{Z}/3\mathbb{Z}$ gilt. Sein nun also eine Dezimalzifferndarstellung von a gegeben durch

$$a_n a_{n-1} \dots a_1 a_0.$$

Das bedeutet gerade

$$a = a_0 + 10 \cdot a_1 + 100 \cdot a_2 + \dots + (10)^n \cdot a_n,$$

und die Quersumme von a ist

$$a_0 + a_1 + \dots + a_n.$$

In $\mathbb{Z}/3\mathbb{Z}$ gilt nun

$$[a] = [a_0 + 10 \cdot a_1 + 100 \cdot a_2 + \cdots + (10)^n \cdot a_n] = [a_0] + [10][a_1] + \cdots + [10]^n[a_n].$$

Wegen $[10] = [1]$ in $\mathbb{Z}/3\mathbb{Z}$ haben wir also die Gleichung

$$[a] = [a_0] + [a_1] + \cdots + [a_n] = [a_0 + \cdots + a_n].$$

Somit ist $[a] = [0]$ genau dann wenn $[a_0 + \cdots + a_n] = [0]$, und beide Aussagen sind jeweils äquivalent zur Teilbarkeit durch 3. Damit ist der Satz bewiesen.
Da nicht nur in $\mathbb{Z}/3\mathbb{Z}$, sondern auch in $\mathbb{Z}/9\mathbb{Z}$ $[10] = [1]$ gilt, funktioniert das Argument genau gleich für Teilbarkeit durch 9:

Satz 1.2.18. *Eine ganze Zahl ist genau dann durch 9 teilbar, wenn ihre Quersumme durch 9 teilbar ist.*

Um eine weitere Teilbarkeitsregel zu erhalten, verwenden wir die Gleichheit

$$[10] = [-1] \text{ in } \mathbb{Z}/11\mathbb{Z}.$$

Wir schreiben eine ganze Zahl a nun wieder in der Form

$$a = a_0 + 10 \cdot a_1 + (10)^2 \cdot a_2 + \cdots + (10)^n \cdot a_n$$

mit allen $a_i \leq 9$. Es gilt nun

$$[a] = [a_0 - a_1 + a_2 - \cdots + (-1)^n a_n] \quad \text{in } \mathbb{Z}/11\mathbb{Z},$$

wobei wir gerade $[10] = [-1]$ verwenden. Damit haben wir bewiesen:

Satz 1.2.19. *Eine ganze Zahl ist genau dann durch 11 teilbar, wenn ihre alternierende Quersumme durch 11 teilbar ist.*

Beispiel 1.2.20. Wir testen ob 1375 durch 11 teilbar ist. Dazu bilden wir die alternierende Quersumme

$$5 - 7 + 3 - 1 = 0,$$

und die ist offensichtlich durch 11 teilbar. Also auch 1375.
Hingegen ist 232984 nicht durch 11 teilbar, denn $4 - 8 + 9 - 2 + 3 - 2 = 4$, und das ist nicht durch 11 teilbar.

Man könnte auch verwenden, dass $[100] = [1]$ in $\mathbb{Z}/11\mathbb{Z}$ gilt. Man schreibt nun

$$a = a_0 + 100a_1 + (100)^2 a_2 + \cdots + (100)^n a_n$$

mit $a_i \leq 99$. Die a_i sind also gerade die *Zweierblöcke* in der Dezimaldarstellung von a. In $\mathbb{Z}/11\mathbb{Z}$ gilt nun

$$[a] = [a_0 + \cdots + a_n]$$

und somit haben wir bewiesen:

Satz 1.2.21. *Eine ganze Zahl ist genau dann durch 11 teilbar, wenn die Quersumme über die Zweierblöcke in ihrer Dezimaldarstellung durch 11 teilbar ist.*

Beispiel 1.2.22. Die Quersumme der Zweierblöcke von 1375 ist $75+13 = 88$. Für 232984 erhält man

$$84 + 29 + 23 = 136,$$

und iteriert

$$36 + 1 = 37.$$

1.2.4 Der Chinesische Restsatz

Wir nehmen einmal an, dass in einer Wohngemeinschaft drei Personen leben, die in regelmäßigen Abständen morgens duschen möchten. Die WG hat zwar zwei Duschen, aber eben keine drei. Person A duscht nun an Tag 1, und dann immer alle drei Tage. Person B duscht einen Tag später, also am Tag 2, und dann nur alle 7 Tage. Person C schließlich duscht am dritten Tag, und dann alle 4 Tage. Solange höchstens zwei Personen gleichzeitig morgens duschen wollen, geht alles in Ordnung. Problematisch wird es nur, wenn alle 3 Personen gleichzeitig in die Dusche wollen. Nun ist die Frage, ob dieser Fall wirklich eintritt, und wenn ja, wann zum ersten Mal. Wenn nach x Tagen dieser Fall eintritt, dann hat x die Gestalt

$$\begin{aligned} x &= 1 + 3k \\ x &= 2 + 7m \\ x &= 3 + 4n, \end{aligned}$$

mit positiven ganzen Zahl k, m, n. Anders formuliert fragen wir uns also, ob es eine positive Zahl x gibt mit

$$\begin{aligned} x &\equiv 1 \bmod 3 \\ x &\equiv 2 \bmod 7 \\ x &\equiv 3 \bmod 4. \end{aligned}$$

Wir wollen also ein *System linearer Kongruenzen* lösen, in dem im Vergleich zu früher nun verschiedene Modulozahlen n auftauchen, hier etwa $3, 4$ und 7. Der sogenannte *Chinesische Restsatz* gibt uns darüber Auskunft:

Satz 1.2.23 (Chinesischer Restsatz)**.** *Seien $n_1, \ldots, n_k$ paarweise teilerfremde ganze Zahlen. Dann gibt es für beliebige ganze Zahlen $a_1, \ldots, a_k$ ein $x \in \mathbb{Z}$ mit*

$$\begin{aligned} x &\equiv a_1 \ \textit{mod}\ n_1 \\ x &\equiv a_2 \ \textit{mod}\ n_2 \\ &\vdots \\ x &\equiv a_k \ \textit{mod}\ n_k. \end{aligned}$$

Dabei ist x modulo $n_1 n_2 \cdots n_k$ eindeutig bestimmt.

Beweis. Die Vorgehensweise zur Konstruktion von x ist wie folgt: zunächst konstruieren wir ganze Zahlen $b_1, \ldots, b_k$ mit

$$\begin{aligned} b_i &\equiv 1 \mod n_i \\ b_i &\equiv 0 \mod n_j \text{ für } j \neq i. \end{aligned}$$

Wenn wir dann

$$x = a_1 b_1 + \cdots + a_k b_k$$

setzen, löst x offenbar das Gleichungssystem, denn in $\mathbb{Z}/n_i\mathbb{Z}$ gilt

$$\begin{aligned} [x] &= [a_1][b_1] + \cdots + [a_i][b_i] + \cdots + [a_k][b_k] \\ &= [a_1][0] + \cdots + [a_i][1] + \cdots + [a_k][0] \\ &= [a_i]. \end{aligned}$$

Um b_i wie gewünscht zu erhalten setzen wir zunächst

$$\widetilde{b}_i := \prod_{j \neq i} n_j.$$

Dann gilt auf jeden Fall schon $\widetilde{b}_i \equiv 0 \mod n_j$ für $j \neq i$. Außerdem ist

$$\mathrm{ggT}(\widetilde{b}_i, n_i) = 1,$$

weil die n_j ja paarweise teilerfremd waren. Damit ist $\widetilde{b}_i$ aber in $\mathbb{Z}/n_i\mathbb{Z}$ multiplikativ invertierbar, nach Korollar 1.2.11. Also gibt es ein $r_i \in \mathbb{Z}$ mit $r_i \widetilde{b}_i \equiv 1 \mod$

n_i. Es gilt aber $r_i\widetilde{b}_i \equiv 0 \bmod n_j$ für $j \neq i$ weiterhin. Also setzen wir $b_i := r_i\widetilde{b}_i$. Damit ist die Existenz einer Lösung bewiesen.
Wenn x' eine weitere Lösung des Gleichungssystems ist, so ist

$$x - x' \equiv 0 \bmod n_i$$

für alle $i = 1, \ldots, k$. Es wird $x - x'$ also von allen n_i geteilt. Keine zwei der n_i haben aber einen Primfaktor gemeinsam. Die Primfaktorzerlegung von $x - x'$ zeigt also, dass $x - x'$ sogar vom Produkt $n_1 n_2 \cdots n_k$ geteilt wird. Also ist die Lösung modulo $n_1 n_2 \cdots n_k$ eindeutig bestimmt. □

Bemerkung 1.2.24. Der Beweis des Chinesischen Restsatzes enthält auch gleich einen Algorithmus zur Konstruktion einer gesuchten Lösung x. Man setzt zunächst

$$\widetilde{b}_i = \prod_{j \neq i} n_j.$$

Dann invertiert man $\widetilde{b}_i$ in $\mathbb{Z}/n_i\mathbb{Z}$, d.h. man sucht ein $r_i \in \mathbb{Z}$ mit $r_i\widetilde{b}_i \equiv 1 \bmod n_i$. Das geht etwa mit dem Euklidischen Algorithmus, in dem man eine Darstellung

$$r_i\widetilde{b}_i + s_i n_i = 1$$

produziert. Mit $b_i = r_i\widetilde{b}_i$ ist dann

$$x = a_1 b_1 + \cdots + a_n b_n$$

eine Lösung.

Beispiel 1.2.25. Im Duschbeispiel von oben haben wir

$$n_1 = 3, n_2 = 7, n_3 = 4,$$

sowie

$$a_1 = 1, a_2 = 2, a_3 = 3.$$

Da die n_i paarweise teilerfremd sind, ist die Existenz einer Lösung garantiert. Wir erhalten

$$\widetilde{b}_1 = 7 \cdot 4 = 28,\ \widetilde{b}_2 = 3 \cdot 4 = 12,\ \widetilde{b}_3 = 3 \cdot 7 = 21.$$

Es ist bereits $\widetilde{b}_1 \equiv 1 \bmod 3$, also können wir $b_1 = \widetilde{b}_1 = 28$ wählen. Weil

$$\widetilde{b}_2 \equiv 5 \bmod 7$$

gilt, müssen wir hier noch modifizieren. Es gilt $3 \cdot 5 = 15 \equiv 1 \bmod 7$, also wählen wir $r_2 = 3$ und $b_2 = r_2\widetilde{b}_2 = 36$. Schließlich ist $\widetilde{b}_3 = 21 \equiv 1 \bmod 4$ und wir setzen $b_3 = \widetilde{b}_3 = 21$. Dann erhalten wir

$$x = b_1 + 2b_2 + 3b_3 = 28 + 2 \cdot 36 + 3 \cdot 21 = 163$$

als Lösung. Man sieht, dass 163 bei Teilung durch 3 wirklich Rest 1, bei Teilung durch 7 Rest 2, und bei Teilung durch 4 Rest 3 lässt.
Wir wollen noch testen, ob das Duschproblem wirklich zum ersten Mal nach 163 Tagen auftritt. Dazu suchen wir die kleinste positive Lösung des Gleichungssystems. Wir wissen, dass die Lösung modulo $3 \cdot 7 \cdot 4 = 84$ eindeutig bestimmt ist, d.h. die Lösungen sind genau von der Gestalt

$$163 + k \cdot 84, \qquad k \in \mathbb{Z}.$$

Wir können also noch einmal 84 abziehen, und erhalten 79 als kleinste positive Lösung. Damit gibt es am Tag 79 das erste Mal Schwierigkeiten mit der Duschenbenutzung.

Beispiel 1.2.26. Dieses Beispiel soll zeigen, dass die Bedingung an die Teilerfremdheit der n_i im chinesischen Restsatz nicht weggelassen werden kann. Dazu ändere Person B der Wohngemeinschaft plötzlich das Hygieneverhalten deutlich, und dusche alle 2 Tage. Schon die beiden Gleichungen

$$x \equiv 2 \mod 2$$
$$x \equiv 3 \mod 4$$

besitzen keine gemeinsame Lösung. Die erste Gleichung impliziert nämlich dass x gerade, die zweite dass x ungerade ist.

1.2.5 Fehlererkennende Codes

In diesem Abschnitt wollen wir noch eine echte Anwendung des Rechnens in Restklassenringen demonstrieren, die (alte) internationale Standardbuchnummer ISBN-10. Obwohl seit 2007 die sogenannte ISBN-13 verwendet wird, ist die ISBN-10 mathematisch etwas interessanter. Die ISBN-10 ist eine Zahl mit 10 Ziffern

$$z_1 z_2 \cdots z_{10},$$

die Büchern und anderen Veröffentlichungen zugeordnet wird. Dabei enthalten nur die ersten 9 Ziffern Informationen über das Buch, wie etwa Verlag und Herstellungsland. Die letzte Ziffer z_{10} ist eine sogenannte *Prüfziffer*, die zur Fehlererkennung und -korrektur verwendet wird. Sie wird so bestimmt, dass die Gesamtnummer die folgende Gleichung erfüllt:

$$z_1 + 2z_2 + 3z_3 + 4z_4 + \cdots + 9z_9 + 10z_{10} \equiv 0 \mod 11. \tag{1.23}$$

Da $10 \equiv -1 \mod 11$ gilt, kann man das auch folgendermaßen formulieren:

$$z_{10} \equiv z_1 + 2z_2 + 3z_3 + \cdots + 9z_9 \bmod 11.$$

Man berechnet also die Summe $z_1 + 2z_2 + \cdots + 9z_9$ modulo 11, und erhält so z_{10}. Dabei können also Werte von 0 bis 10 für z_{10} auftreten. Damit z_{10} aber immer eine einzelne Ziffer bleibt, verwendet man das Symbol X anstelle von 10.

Beispiel 1.2.27. Die ersten 9 Ziffern der ISBN-10 seien 247810378. Man berechnet

$$1 \cdot 2 + 2 \cdot 4 + 3 \cdot 7 + 4 \cdot 8 + 5 \cdot 1 + 6 \cdot 0 + 7 \cdot 3 + 8 \cdot 7 + 9 \cdot 8 = 217.$$

Wegen $217 \equiv 8 \mod 11$ erhält man also $z_{10} = 8$ und somit die ISBN-10 Nummer

$$2478103788.$$

Wäre die zweite Ziffer eine 5 gewesen, hätte die Summe 219 ergeben, und $219 \equiv 10 \mod 11$. Man hätte $z_{10} = \mathrm{X}$ und damit

$$257810378\mathrm{X}$$

erhalten.

Das Anfügen einer Prüfziffer dient dem Erkennen und eventuellem Korrigieren einer falschen ISBN Nummer. Ist zum Beispiel eine Ziffer unlesbar, geht dadurch keine Information verloren. Es gilt nämlich:

Lemma 1.2.28. *Jeder der zehn Ziffern z_i ist durch die Gleichung 1.23 eindeutig durch die anderen Ziffern bestimmt. Insbesondere kann eine fehlende Ziffer immer mit Hilfe der anderen rekonstruiert werden.*

Beweis. Für ein festes $1 \leq i \leq 10$ lösen wir Gleichung 1.23 nach dem Term iz_i auf:

$$iz_i \equiv -\sum_{j \neq i} jz_j \bmod 11.$$

Wenn wir alle z_j mit $j \neq i$ kennen, haben wir es also mit einer Gleichung

$$[i][z_i] = [b]$$

in $\mathbb{Z}/11\mathbb{Z}$ zu tun. Da $[i]$ in $\mathbb{Z}/11\mathbb{Z}$ nach Satz 1.2.13 multiplikativ invertierbar ist, kennen wir somit $[z_i]$ in $\mathbb{Z}/11\mathbb{Z}$. Da z_i eine Ziffer ist, also zwischen 0 und 9 liegt (im Falle $i = 10$ zwischen 0 und 10), ist es damit eindeutig bestimmt. □

Korollar 1.2.29. *Wird in einer gültigen ISBN-Nummer genau eine Ziffer abgeändert, so ist die Prüfgleichung 1.23 nicht mehr erfüllt.*

Beweis. Wenn durch das Abändern einer Ziffer erneut eine Nummer entstünde, die 1.23 erfüllt, wäre damit die Eindeutigkeit aus Lemma 1.2.28 widerlegt. □

Wenn also durch ein Versehen eine Ziffer einer ISBN-Nummer falsch wiedergegeben wird, so wird dieser Fehler durch das Überprüfen der Gleichung 1.23 auf jeden Fall entdeckt. Natürlich stimmt das im Allgemeinen nicht mehr, wenn mehrere Ziffern gleichzeitig Fehler enthalten. Wird zum Beispiel z_1 um zwei erhöht und gleichzeitig z_2 um eins verringert, gilt Gleichung 1.23 auch hinterher wieder, und der Fehler wird nicht bemerkt. Anders ist das allerdings, wenn zwei Ziffern versehentlich vertauscht werden (was zum Beispiel beim Abtippen leicht passiert):

Lemma 1.2.30. *Werden in einer gültigen ISBN-Nummer zwei verschiedene Ziffern vertauscht, ist die Prüfgleichung 1.23 nicht mehr erfüllt.*

Beweis. Angenommen die Ziffern z_j und z_k werden vertauscht, wobei $z_j \neq z_k$. Die Summe auf der linken Seite der Prüfgleichung war vorher

$$\sum_{i=1}^{10} iz_i,$$

und ist hinterher

$$\sum_{i \neq j,k} iz_i + jz_k + kz_j.$$

Die Differenz der beiden Summen ist also gerade

$$jz_j + kz_k - jz_k - kz_j = (j-k)z_j + (k-j)z_k = (j-k)(z_j - z_k).$$

Offensichtlich ist 11 aber kein Teiler dieser Differenz. Schließlich ist 11 prim und müsste nach Satz 1.1.27 sonst einen der beiden Faktoren teilen. Diese Faktoren sind aber jeweils kleiner gleich 10.

Da die ursprüngliche Summe durch 11 teilbar war, die Differenz aber nicht, kann die neue Summe nicht durch 11 teilbar sein. Damit ist die Prüfgleichung für die fehlerhafte Nummer nicht erfüllt. □

1.3 Die rationalen Zahlen $\mathbb{Q}$

Das Glück ist das einzige, das sich verdoppelt, wenn man es teilt.

Albert Schweizer (1875-1965)

... und die Null!

Anonymer Mathematiker

... also: Glück = Null!

Anonymer Zen-Mönch

1.3.1 Konstruktion und Eigenschaften

In den ganzen Zahlen $\mathbb{Z}$ sind viele Gleichungen der Gestalt

$$a \cdot x = b$$

nicht lösbar, da man beispielsweise nicht einfach durch a teilen kann. Um dieses Problem zu beheben, geht man zu den *rationalen Zahlen* über, die mit $\mathbb{Q}$ bezeichnet werden. Wir wollen zunächst eine auf den ganzen Zahlen aufbauende und mathematisch genaue Definition der rationalen Zahlen angeben. Dazu definieren wir eine Äquivalenzrelation auf der Menge $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ wie folgt:

$$(a, b) \sim (c, d) \quad :\Leftrightarrow \quad ad = bc.$$

Ist ist also beispielsweise $(1, 2) \sim (2, 4)$. Es gilt

Lemma 1.3.1. *Die Relation $\sim$ ist eine Äquivalenzrelation auf $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$.*

Beweis. Es gilt $(a,b) \sim (a,b)$, da $ab = ba$. Falls $(a,b) \sim (c,d)$, so auch $(c,d) \sim (a,b)$, denn $ad = bc$ impliziert $cb = da$. Es gelte schließlich $(a,b) \sim (c,d)$ und $(c,d) \sim (e,f)$, also $ad = bc$ und $cf = de$. Wir multiplizieren die erste Gleichung mit f und die zweite mit b, und erhalten $adf = bcf$ sowie $bcf = bde$. Das impliziert $adf = bde$, und mit der Kürzungsregel $af = be$. Dabei verwenden wir $d \neq 0$. Das bedeutet $(a,b) \sim (e,f)$. □

Man beachte dass wir die Kürzungsregel für die Transitivität verwendet haben. In $\mathbb{Z}/n\mathbb{Z}$ wäre das nicht ohne weiteres möglich. Wir bezeichnen nun mit $[(a,b)]$ die Äquivalenzklasse von (a,b) bezüglich $\sim$. Die Menge aller Äquivalenzklassen nennen wir die *rationalen Zahlen*:

$$\mathbb{Q} = \{[(a,b)] \mid (a,b) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})\}.$$

Im nächsten Schritt definieren wir Addition und eine Multiplikation auf $\mathbb{Q}$. Das wird wie in $\mathbb{Z}/n\mathbb{Z}$ anhand von Vertretern der Äquivalenzklasse gemacht, und benötigt dann einen Beweis der Wohldefiniertheit. Zunächst die Definition:

$$[(a,b)] + [(c,d)] := [(ad + bc, bd)]$$

$$[(a,b)] \cdot [(c,d)] := [(ac, bd)]$$

Man beachte dass aufgrund der Nullteilerfreiheit von $\mathbb{Z}$ immer $bd \neq 0$ ist, wenn $b, d \neq 0$.

Lemma 1.3.2. *Die Verknüpfungen $+$ und $\cdot$ sind wohldefiniert auf $\mathbb{Q}$, d.h. unabhängig von den Vertretern der Äquivalenzklassen.*

Beweis. Sei $[(a,b)] = [(a',b')]$ und $[(c,d)] = [(c',d')]$. Es gilt also $ab' = ba'$ und $cd' = dc'$. Wir müssen zeigen dass

$$[(ad + bc, bd)] = [(a'd' + b'c', b'd')]$$

gilt, also gerade

$$(ad + bc)b'd' = bd(a'd' + b'c').$$

Wenn wir aber die Gleichung $ab' = ba'$ mit dd' und die Gleichung $cd' = dc'$ mit bb' multiplizieren und beide aufaddieren, erhalten wir genau das gewünschte Resultat. Für die Multiplikation müssen wir $[(ac, bd)] = [(a'c', b'd')]$ zeigen, also

$$acb'd' = bda'c'.$$

Wenn wir die erste der oberen Gleichungen mit cd' und die zweite mit ba' multiplizieren, sind jeweils zwei Seiten gleich. Durch Gleichsetzen der anderen Seiten erhalten wir das Ergebnis. □

Satz 1.3.3. *Für das Rechnen in $\mathbb{Q}$ gelten die Regeln (1.1)-(1.8) aus dem ersten Abschnitt. Dabei ist $[(0,1)]$ das neutrale Element bezüglich $+$, und $[(1,1)]$ das neutrale Element bezüglich $\cdot$. Die ganzen Zahlen $\mathbb{Z}$ lassen sich vermöge der Zuordnung $a \mapsto [(a,1)]$ in $\mathbb{Q}$ einbetten; die Verknüpfungen in $\mathbb{Q}$ entsprechen dann genau den bekannten Verknüpfungen in $\mathbb{Z}$.*

Beweis. Die Eigenschaften (1.1)-(1.8) lassen sich leicht, aber etwas zeitaufwändig nachrechnen. Dabei verwendet man immer wieder, dass die Eigenschaften in $\mathbb{Z}$ gelten. Es gilt zum Beispiel

$$[(a,b)] + [(0,1)] = [(a \cdot 1 + b \cdot 0, b \cdot 1)] = [(a,b)]$$

und

$$[(a,b)] \cdot [(1,1)] = [(a \cdot 1, b \cdot 1)] = [(a,b)].$$

Die Zuordnung $a \mapsto [(a,1)]$ ist eine Einbettung, d.h. injektiv: aus $[(a,1)] = [(b,1)]$ folgt $a \cdot 1 = 1 \cdot b$, d.h $a = b$. Es gilt nun

$$[(a,1)] + [(b,1)] = [(a+b,1)]$$

und

$$[(a,1)] \cdot [(b,1)] = [(ab,1)].$$

Für ganze Zahlen sind die neuen Verknüpfungen also gerade die alten. □

Wir können nun alle ganze Zahlen a mit ihrem Bild $[(a,1)]$ in $\mathbb{Q}$ identifizieren, und so $\mathbb{Z}$ als *Teilmenge* von $\mathbb{Q}$ auffassen:

$$\mathbb{Z} \subseteq \mathbb{Q}.$$

Außerdem hat sich die Schreibweise

$$\frac{a}{b}$$

für die Äquivalenzklasse $[(a,b)]$ eingebürgert. Dabei muss man aber im Hinterkopf behalten, dass es sich immer noch um eine Äquivalenzklasse handelt. Es gilt also

$$\frac{a}{b} = \frac{c}{d} \Leftrightarrow ad = bc.$$

Man überprüfe wie die Definition von $+$ und $\cdot$ in der Bruchschreibweise aussieht! Für ganze Zahlen a schreibt man auch weiterhin oft nur a anstatt $\frac{a}{1}$ oder $[(a,1)]$. So bezeichnet $0 = [(0,1)]$ das neutrale Element bezüglich $+$ und $1 = [(1,1)]$ das neutrale Element bezüglich $\cdot$.

Lemma 1.3.4. *In $\mathbb{Q}$ gilt die Nullteilerfreiheit, und damit die Kürzungsregel.*

Beweis. Es gelte $0 = [(0,1)] = [(a,b)] \cdot [(c,d)] = [(ac,bd)]$. Nach Definition bedeutet das

$$0 \cdot bd = 1 \cdot ac.$$

Aus der Nullteilerfreiheit von $\mathbb{Z}$ folgt o.B.d.A $a = 0$, und damit

$$[(a,b)] = [(0,b)] = [(0,1)] = 0,$$

denn $0 \cdot 1 = b \cdot 0$. Die Kürzungsregel folgt aus der Nullteilerfreiheit wie in Lemma 1.1.4. □

Der folgende Satz demonstriert die wichtigste Eigenschaft von $\mathbb{Q}$ gegenüber $\mathbb{Z}$:

Satz 1.3.5. *Für $a, b \in \mathbb{Q}$, $a \neq 0$ hat die Gleichung*

$$a \cdot x = b$$

genau eine Lösung $x \in \mathbb{Q}$.

Beweis. Schreibe $a = [(r,s)]$ und $b = [(t,u)]$ mit $r, s, t, u \in \mathbb{Z}, s, u \neq 0$. Dabei bedeutet $a \neq 0$ gerade $r \neq 0$. Setze

$$x = [(st, ru)].$$

Das ist wohldefiniert, denn $ru \neq 0$. Wir rechnen nun

$$a \cdot x = [(r,s)] \cdot [(st,ru)] = [(rst, sru)].$$

Es gilt aber $[(rst, sru)] = [(t,u)] = b$, denn $rstu = srut$. Also ist die Gleichung lösbar. Die Eindeutigkeit folgt direkt aus der Kürzungsregel. □

Korollar 1.3.6. *In $\mathbb{Q}$ besitzt jedes Element $a \neq 0$ ein eindeutig bestimmtes multiplikativ inverses Element.*

Beweis. Das ist gerade Satz 1.3.5 mit $b = 1$. □

Wir bezeichen das multiplikativ inverse Element zu a mit a^{-1}. Falls $a = [(r,s)]$ so gilt $a^{-1} = [(s,r)]$, wie man dem Beweis von Satz 1.3.5 sofort entnimmt. Daraus folgt zum Beispiel sofort

$$(ab)^{-1} = b^{-1}a^{-1} \text{ und } (a^{-1})^{-1} = a.$$

1.3.2 Zwei Irrationalitätsbeweise

Wir haben gesehen, dass man in $\mathbb{Q}$ sehr viel mehr Gleichungen lösen kann als beispielsweise in $\mathbb{Z}$. Trotzdem gibt es immer noch Gleichungen, die unlösbar sind, zum Beispiel

$$x^2 - 2 = 0.$$

Satz 1.3.7. *Es gibt keine rationale Zahl $a \in \mathbb{Q}$ mit $a \cdot a = 2$.*

Beweis. Wir nehmen an es gebe $a = \frac{s}{t}$ mit $a^2 = 2$. Das bedeutet $2 = \frac{2}{1} = \frac{s^2}{t^2}$, also

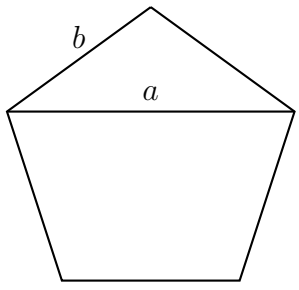
$$2t^2 = s^2. \tag{1.24}$$

Da die Primzahl 2 das Produkt s^2 teilt, teilt sie schon s. Kürzen wir nun 2 auf beiden Seiten in 1.24 erhalten wir

$$t^2 = 2\tilde{s}^2,$$

wobei $2\tilde{s} = s$. Das Argument lässt sich nun beliebig oft wiederholen, und zeigt, dass 2 in beliebig hohen Potenzen als Faktor von t und s auftaucht. Das ist ein Widerspruch zu Satz 1.1.28, da $t \neq 0$. □

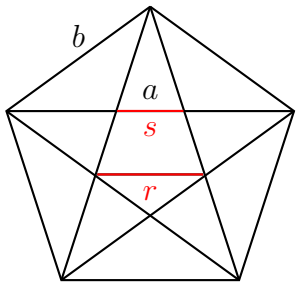
Die Aussage des letzten Satzes wird oft als *Irrationalität von $\sqrt{2}$* zusammengefasst. Hat man einmal die reellen Zahlen $\mathbb{R}$ konstruiert, und dort eine Wurzel aus 2 gefunden, kann man sagen, dass $\sqrt{2}$ eine reelle, aber keine rationale Zahl ist. Solange man die reellen Zahlen aber nicht kennt (wie zum Beispiel die Griechen), ist diese Irrationalitätsaussage problematisch. $\sqrt{2}$ ist dann nämlich nicht einfach irrational, sondern *existiert nicht*. Die Formulierung von Satz 1.3.7 vermeidet deshalb einen Rückgriff auf $\mathbb{R}$.
Noch etwas deutlicher wird das Problem im folgenden Beispiel. Man betrachte ein regelmäßiges Fünfeck mit Diagonallänge a und Seitenlänge b:



Wir wollen nun zeigen, dass a und b in keinem rationalen Verhältnis zueinander stehen. Kennt man wiederum die reellen Zahlen bereits, könnte man sagen, dass $ab^{-1} \in \mathbb{R} \setminus \mathbb{Q}$ gilt. Da wir die reellen Zahlen noch nicht eingeführt haben, können wir dies nicht. Inbesondere ist der Ausdruck ab^{-1} eventuell überhaupt nicht definiert. Die einzig sinnvolle Aussage die wir treffen können, und die auch die Griechen bereits getroffen haben, ist die folgende. Dabei verwenden wir die geometrische Variante des Euklidischen Algorithmus aus Abschnitt 1.1.3:

Satz 1.3.8. *Die Streckenlängen a und b verhalten sich nicht zueinander wie zwei ganze Zahlen.*

Beweis. Angenommen, a und b verhielten sich doch zueinander wie zwei ganze Zahlen. Dann würde der Euklidische Algorithmus, angewandt auf a und b, nach endlich vielen Schritten abbrechen (Satz 1.1.12). Wir wenden den Algorithmus nun geometrisch an, und betrachten zunächst alle Diagonalen im Fünfeck. Dabei entsteht im Inneren ein weiteres regelmäßiges Fünfeck, dessen Diagonale r und Seite s wir ebenfalls betrachten:



Man sieht nun leicht, dass b einmal voll in a passt, und gerade r als Rest lässt:

$$a = b + r.$$

Dies ist der erste Schritt im Euklidischen Algorithmus. Für den zweiten tragen wir r einmal in b ab und erhalten s als Rest:

$$b = r + s.$$

Im dritten Schritt muss man also den Euklidischen Algorithmus auf r und s anwenden. Das sind aber gerade wieder Diagonale und Seite in einem regelmäßigen Fünfeck! Nach drei Schritten ist man also wieder am Ausgangspunkt angekommen und sieht, dass der Algorithmus nicht nach endlich vielen Schritten abbrechen wird. Also standen a und b nicht im Verhältnis zweier ganzer Zahlen zueinander. □

Die Griechen hat dieses Ergebnis stark irritiert. Sie kannten nur die rationalen Zahlen, also die Verhältnisse von ganzen Zahlen. Somit standen a und b nicht nur nicht im Verhältnis wie zwei ganze Zahlen, sie standen *in gar keinem Verhältnis*. Das dürfte ihnen sehr merkwürdig vorgekommen sein, insbesondere da man beide Strecken mit Zirkel und Lineal konstruieren, und deshalb wirklich „sehen" kann. Wir wollen dieses Phänomen zum Anlass nehmen, uns näher mit den reellen Zahlen zu beschäftigen. Obwohl wir sie seit der Schule gewöhnlich als völlig selbstverständlich betrachten, sind sie doch eine höchst abstrakte Konstruktion, deren exakte Formulierung die Mathematiker bis Ende des 19. Jahrhunderts beschäftigte.

1.4 Die reellen Zahlen $\mathbb{R}$

> *So kann also die Mathematik definiert werden als diejenige Wissenschaft, in der wir niemals das kennen, worüber wir sprechen, und niemals wissen, ob das, was wir sagen, wahr ist.*
>
> Bertrand Russell (1872-1970)

1.4.1 Konstruktion und Eigenschaften

Wir haben gesehen, dass die rationalen Zahlen für das Lösen von gewissen Gleichungen noch nicht ausreichen. Ein Beispiel ist die Gleichung $x^2 - 2 = 0$. Deshalb erweitern wir den bisherigen Zahlbereich $\mathbb{Q}$ weiter zu den sogenannten *reellen Zahlen* $\mathbb{R}$. Eine der heute geläufigsten Methoden hierfür verwendet Cauchyfolgen. Eine Folge $(a_n)_{n\in\mathbb{N}}$ von *rationalen* Zahlen heißt *Cauchyfolge*, wenn sie die folgende Bedingung erfüllt:

$$\forall N \in \mathbb{N} \quad \exists m \in \mathbb{N} \quad \forall n, n' \geq m\colon \quad |a_n - a_{n'}| \leq \frac{1}{N}.$$

Etwas salopper in Worten: *Die Folgenglieder unterscheiden sich für großen Folgenindex kaum noch voneinander.* Wir erinnern auch noch einmal an den Begriff einer *konvergenten Folge*:

$$\exists a \in \mathbb{Q} \quad \forall N \in \mathbb{N} \quad \exists m \in \mathbb{N} \quad \forall n \geq m\colon \quad |a - a_n| \leq \frac{1}{N}.$$

In Worten: *Die Folgenglieder kommen für großen Folgenindex der Zahl a beliebig nahe.*

Es ist leicht zu sehen, dass konvergente Folgen immer Cauchyfolgen sind. Im Unterschied zur konvergenten Folge nimmt der Begriff der Cauchyfolge aber nicht Bezug auf einen Grenzwert. Der Grund dafür ist, dass es Folgen gibt, die sich eigentlich wie konvergente Folgen verhalten, aber trotzdem keinen Grenzwert besitzen:

Beispiel 1.4.1. Wir betrachten die Folge $(a_n)_{n\in\mathbb{N}}$ rationaler Zahlen, die folgendermaßen rekursiv definiert ist:

$$a_1 = 2,\ a_{n+1} = \frac{1}{2}\left(a_n + \frac{2}{a_n}\right).$$

Dem liegt eine einfache geometrische Idee zugrunde. Wir möchten ein Quadrat mit Flächeninhalt 2 konstruieren. Das hat dann eine Seitenlänge, die quadriert 2 ergibt. Wir starten allerdings mit einem sehr einfachen *Rechteck* mit Flächeninhalt 2. Wir nehmen einfach die Seitenlängen

$$a_1 = 2 \text{ und } b_1 = 1 = \frac{2}{a_1}.$$

Im nächsten Schritt machen wir das Rechteck ein wenig mehr zu einem Quadrat, indem wir die längere Seite a_1 durch das Mittel der beiden Seiten a_1 und b_1 ersetzen:

$$a_2 = \frac{1}{2}(a_1 + b_1) = \frac{1}{2}\left(a_1 + \frac{2}{a_1}\right),$$

und als zweite Seite wieder $b_2 = \frac{2}{a_2}$ nehmen. Dieser Prozess wird iteriert. Da das Rechteck dabei immer Flächeninhalt 2 hat, und einem Quadrat immer ähnlicher wird, konvergieren die Seiten gegen eine Streckenlänge x, die $x^2 = 2$ erfüllt.
Man kann allerdings auch ganz formal zeigen, dass die Folge $(a_n)_n$ eine Cauchyfolge in $\mathbb{Q}$ ist, die in $\mathbb{Q}$ aber keinen Grenzwert besitzt, da dieser $x^2 = 2$ erfüllen würde. Die Folge $(a_n^2)_n$ hingegen konvergiert in $\mathbb{Q}$, und zwar gegen 2.

Cauchyfolgen sind also Folgen, die sich genau wie konvergente Folgen verhalten, nur eben nicht unbedingt einen Grenzwert haben. Man möchte das Problem des fehlenden Grenzwertes nun beheben. Aber wo bekommt man einen Grenzwert her? Die geniale Idee ist, die Cauchyfolge *selbst* als ihren eigenen Grenzwert zu verwenden. Bezeichne $\mathcal{C}$ die Menge aller Cauchyfolgen rationaler Zahlen:

$$\mathcal{C} := \{(a_n)_{n\in\mathbb{N}} \mid (a_n)_{n\in\mathbb{N}} \text{ Cauchyfolge, alle } a_n \in \mathbb{Q}\}.$$

Wir definieren eine Äquivalenzrelation auf $\mathcal{C}$ durch

$$(a_n)_n \sim (b_n)_n : \Leftrightarrow (a_n - b_n)_n \text{ konvergiert gegen } 0.$$

Man rechnet nach, dass $\sim$ wirklich eine Äquivalenzrelation ist. Wir gehen nun wie üblich zu Äquivalenzklassen über, identifizieren also äquivalente Folgen. Die Restklassen bilden dann die reellen Zahlen

$$\mathbb{R} := \{[(a_n)_n] \mid (a_n)_n \in \mathcal{C}\}.$$

Man definiert $+$ und $\cdot$ glied- und vertreterweise:

$$[(a_n)_n] + [(b_n)]_n := [(a_n + b_n)_n]$$

$$[(a_n)_n] \cdot [(b_n)]_n := [(a_n \cdot b_n)_n],$$

wobei wieder einiges zur Wohldefiniertheit zu zeigen ist. Man erhält dann wieder alle Eigenschaften (1.1)-(1.8), mit den neutralen Elementen $[(0)_n]$ und $[(1)_n]$. Jedes Element $[(a_n)_n] \neq 0$ ist außerdem multiplikativ invertierbar. Wenn nämlich $(a_n)_n$ eine Cauchyfolge, aber keine Nullfolge ist, dann können wir zunächst $a_n \neq 0$ für alle $n \in \mathbb{N}$ annehmen (Änderungen an endlich vielen Stellen ändern die Äquivalenzklasse bezüglich $\sim$ nicht). Weiter ist $(\frac{1}{a_n})_n$ wieder eine Cauchyfolge (hier wird nochmals verwendet, dass $(a_n)_n$ keine Nullfolge ist!), und die Restklasse $[(\frac{1}{a_n})_n]$ ist dann offensichtlich multiplikativ invers zu $[(a_n)_n]$.
Man kann auch die Anordnung $\leq$, die man für die Definition von Cauchyfolgen und konvergenten Folgen benötigt, auf $\mathbb{R}$ definieren:

$$[(a_n)_n] < [(b_n)_n] : \Leftrightarrow \exists N, M \in \mathbb{N} \quad \forall m \geq M : \quad a_m + \frac{1}{N} < b_m.$$

Man bettet $\mathbb{Q}$ in $\mathbb{R}$ ein, indem man $a \in \mathbb{Q}$ mit der Restklasse der konstanten Folge $(a)_n$ identifiziert:

$$a = [(a)_{n \in \mathbb{N}}].$$

Wiederum stimmen die neu definierten Verknüpfungen mit den alten auf $\mathbb{Q}$ überein. So kann man also sinnvollerweise $\mathbb{Q} \subset \mathbb{R}$ schreiben.
Erstaunlicherweise haben nun rationale Cauchyfolgen *immer* einen Grenzwert in $\mathbb{R}$. Sei nämlich $(a_n)_n$ eine Cauchyfolge in $\mathbb{Q}$. Zunächst fassen wir jedes Folgenglied a_n als reelle Zahl auf, d.h. als Äquivalenzklasse der konstanten Folge:

$$a_n = [(a_n)_m] \in \mathbb{R}.$$

Wir wollen zeigen, dass die *Folge* der a_n in $\mathbb{R}$ gegen das *Element* $[(a_m)_m] \in \mathbb{R}$ konvergiert. Dazu bilden wir für festes n die Differenz

$$[(a_m)_m] - a_n = [(a_m)_m] - [(a_n)_m] = [(a_m - a_n)_m].$$

Da die ursprüngliche Folge eine Cauchyfolge war, sind die Zahlen $a_m - a_n$ beliebig klein, wenn nur m und n groß genug sind. Daraus folgt die gewünschte Konvergenz, wie man sich unter Zuhilfenahme der Definition von $<$ auf $\mathbb{R}$ überlegt.

Beispiel 1.4.2. Die Folge $(a_n)_n$ aus Beispiel 1.4.1 besitzt einen Grenzwert in $\mathbb{R}$, und zwar gerade das Element $x = [(a_n)_n]$. Wir berechnen nun x^2 in $\mathbb{R}$:

$$x^2 = [(a_n)_n] \cdot [(a_n)_n] = [(a_n^2)_n].$$

Da die Folge $(a_n^2)_n$ in $\mathbb{Q}$ gegen 2 konvergiert, ist die Folge $(2 - a_n^2)_n$ eine Nullfolge. Damit gilt $(a_n^2)_n \sim (2)_n$, und also

$$x^2 = [(a_n^2)_n] = [(2)_n] = 2.$$

Somit haben wir in x eine Wurzel aus 2 gefunden, die wir fortan mit $\sqrt{2}$ bezeichnen.

Man kann sogar zeigen, das Cauchyfolgen *reeller Zahlen* in $\mathbb{R}$ immer einen Grenzwert besitzen. Wir haben das nur für Cauchyfolgen *rationaler Zahlen* gezeigt, wollen es aber hier auch nicht weiter vertiefen.
Wir können in $\mathbb{R}$ also noch deutlich mehr Gleichungen als in $\mathbb{Q}$ lösen. Vollständig zufrieden sind wir aber immer noch nicht:

Lemma 1.4.3. *Die Gleichung $x^2 + 1 = 0$ besitzt keine Lösung in $\mathbb{R}$.*

Beweis. Angenommen $x = [(a_n)_n] \in \mathbb{R}$ erfülle

$$0 = x^2 + 1 = [(a_n^2 + 1)_n].$$

Das bedeutet dass $(a_n^2 + 1)_n$ eine Nullfolge ist. Das kann aber nicht sein, da $a_n^2 + 1 \geq 1$ in $\mathbb{Q}$ gilt. □

Nachdem wir uns bisher unlösbare Gleichungen zum Anlass genommen haben, unseren Zahlbereich zu erweitern, wollen wir das auch diesmal tun. Wir konstruieren also die *komplexen Zahlen*. Der Fundamentalsatz der Algebra wird uns dann zeigen, dass wir damit in gewisser Weise an ein natürliches Ende des Erweiterungsprozesses gekommen sind.

1.5 Die komplexen Zahlen $\mathbb{C}$

Es gibt Dinge, die den meisten Menschen unglaublich erscheinen, die nicht Mathematik studiert haben.

Archimedes (287-212 v. Chr.)

1.5.1 Konstruktion

Wir möchten nun eine Lösung für eine bisher unlösbare Gleichung finden, nämlich für $x^2 + 1 = 0$. Wir benötigen also eine Quadratwurzel aus -1. In den sogenannten *komplexen Zahlen* werden wir eine solche finden. Als Menge sind die komplexen Zahlen einfach die reelle Ebene $\mathbb{R}^2$:

$$\mathbb{C} = \mathbb{R} \times \mathbb{R} = \{(a, b) \mid a, b \in \mathbb{R}\}.$$

Wir definieren nun Addition und Multiplikation wie folgt:

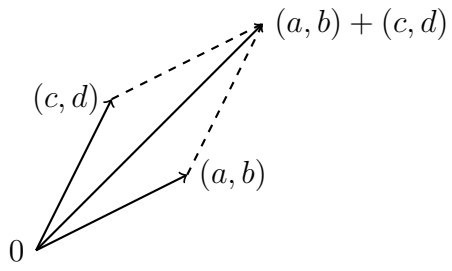
$$(a, b) + (c, d) = (a + c, b + d)$$

$$(a, b) \cdot (c, d) = (ac - bd, ad + bc).$$

Es ist also beispielsweise

$$(3, -2) + (2, 1) = (5, -1), \quad (3, -2) \cdot (2, 1) = (8, -1).$$

Die Addition entspricht also einfach dem Addieren von Vektoren des $\mathbb{R}^2$:



Wir werden später sehen, dass auch die Multiplikation eine geometrische Interpretation besitzt.

Satz 1.5.1. *Für das Rechnen in $\mathbb{C}$ gelten die Regeln (1.1)-(1.8) aus dem ersten Abschnitt. Dabei ist $(0,0)$ das additiv neutrale, und $(1,0)$ das multiplikativ neutrale Element. Das additiv inverse Element zu (a,b) ist $(-a,-b)$. Jedes Element $z=(a,b)\neq(0,0)$ besitzt ein eindeutiges multiplikativ Inverses:*

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

Beweis. Wir rechnen nur einige Aussagen nach, der Rest ist Übungsaufgabe. Zum Beispiel ist

$$(a,b)+(0,0)=(a+0,b+0)=(a,b)$$

und

$$(a,b)\cdot(1,0)=(a\cdot 1-b\cdot 0,a\cdot 0+b\cdot 1)=(a,b).$$

Weiter gilt

$$\begin{aligned}(a,b)\cdot\left(\frac{a}{a^2+b^2},\frac{-b}{a^2+b^2}\right)&=\left(\frac{a^2}{a^2+b^2}-\frac{-b^2}{a^2+b^2},\frac{-ab}{a^2+b^2}+\frac{ab}{a^2+b^2}\right)\\&=\left(\frac{a^2+b^2}{a^2+b^2},0\right)=(1,0).\end{aligned}$$

□

Wir betten nun $\mathbb{R}$ in $\mathbb{C}$ ein, indem wir $a\in\mathbb{R}$ mit $(a,0)\in\mathbb{C}$ identifizieren. Wir identifizieren $\mathbb{R}$ also mit der x-Achse in $\mathbb{R}^2$. Die neuen Verknüpfungen stimmen dann gerade mit den alten überein:

$$(a,0)+(b,0)=(a+b,0),\quad (a,0)\cdot(b,0)=(ab-0\cdot 0,a\cdot 0+b\cdot 0)=(ab,0).$$

Das additiv neutrale Element ist also gerade die alte 0, das multiplikativ neutrale ist die alte 1. Besonders interessant ist nun das Element $(0,1)$, das nicht zu den reellen Zahlen gehört. Wir rechnen

$$(0,1)\cdot(0,1)=(0\cdot 0-1\cdot 1,0\cdot 1+1\cdot 0)=(-1,0)=-1\in\mathbb{R}.$$

Wir haben also eine Quadratwurzel aus -1 gefunden, die selbst allerdings keine reelle Zahl ist.
Gewöhnlich werden komplexe Zahlen $z=(a,b)$ nicht als Tupel geschrieben, sondern in der Form

$$z=a+bi.$$

Dabei ist

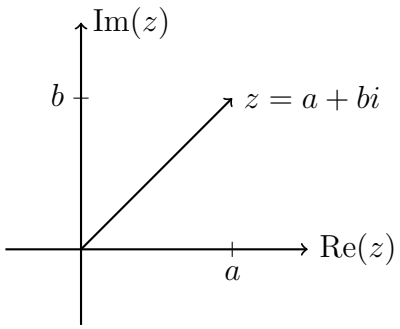
$$i = 0 + 1 \cdot i = (0, 1)$$

und es gilt

$$i^2 = -1.$$

Die Zahl a heißt *Realteil,* und b *Imaginärteil* von z. Wir schreiben auch

$$\mathrm{Re}(z) = a, \quad \mathrm{Im}(z) = b.$$



Die Schreibweise $a + bi$ hat den Vorteil, dass wir vor allem Produkte leichter ausrechnen können. Wir müssen uns nicht die Formel merken, sondern dürfen das Distributivgesetz verwenden, und müssen nur $i^2 = -1$ im Kopf behalten:

$$\begin{aligned}(a, b) \cdot (c, d) &= (a + bi) \cdot (c + di) = ac + adi + bci + bdi^2 \\ &= ac - bd + (ad + bc)i = (ac - bd, ad + bc).\end{aligned}$$

In dieser Schreibweise haben wir also

$$(a + bi)^{-1} = \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2} i.$$

Beispiel 1.5.2. Wir wollen einige Beispielrechnungen mit komplexen Zahlen durchführen:

$$(3 + 2i) + (-5 + i) = -2 + 3i$$

$$-(5 - 2i) = -5 + 2i$$

$$(5 - 2i) + (-5 + 2i) = 5 - 5 + (-2 + 2)i = 0 + 0i = 0$$

$$(1 + i) \cdot (1 - i) = 1 - i + i - i^2 = 1 + 1 = 2$$

$$(1+i)^{-1} = \frac{1}{2} - \frac{1}{2}i$$
$$(1+i)\cdot\left(\frac{1}{2} - \frac{1}{2}i\right) = \frac{1}{2} - \frac{1}{2}i + \frac{1}{2}i - \frac{1}{2}i^2 = \frac{1}{2} + \frac{1}{2} = 1.$$

Beispiel 1.5.3. Wir wollen die Gleichung

$$(1+i)\cdot z = i$$

in $\mathbb{C}$ lösen. Dazu multiplizieren wir mit dem Inversen von $1+i$ auf beiden Seiten. Das Inverse ist $\frac{1}{2} - \frac{1}{2}i$, wie wir im letzten Beispiel gesehen haben. Es ergibt sich

$$z = \left(\frac{1}{2} - \frac{1}{2}i\right)\cdot i = \frac{1}{2}i - \frac{1}{2}i^2 = \frac{1}{2} + \frac{1}{2}i$$

als Lösung.

Beispiel 1.5.4. Wir wollen die Gleichung

$$z^2 = -5$$

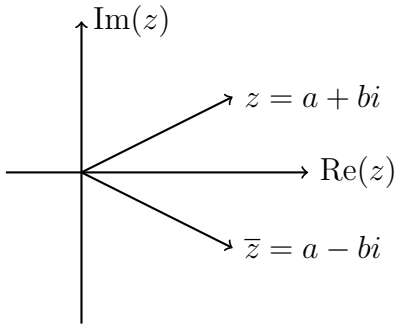
lösen. Wir wissen schon, dass $i^2 = -1$ gilt. Damit folgt mit $z = \sqrt{5}i$

$$z^2 = \sqrt{5}^2 i^2 = -5.$$

Auf den komplexen Zahlen gibt es eine weitere nützliche Operation, die sogenannte *komplexe Konjugation*. Für eine komplexe Zahl $z = a + bi = (a, b)$ heißt

$$\overline{z} = a - bi = (a, -b)$$

die komplex konjugierte Zahl. Sie entsteht gerade durch Multiplikation des Imaginärteils mit -1. Geometrisch handelt es sich dabei um Spiegelung an der x-Achse:



Satz 1.5.5. *Für komplexe Zahlen z, z_1, z_2 gilt:*

(i) $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$

(ii) $\overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2}$

(iii) $\overline{z^{-1}} = (\overline{z})^{-1}$

(iv) $z = \overline{z} \Leftrightarrow z \in \mathbb{R}$

(v) $\overline{\overline{z}} = z$

(vi) $\mathrm{Re}(z) = \frac{1}{2}(z + \overline{z})$ *und* $\mathrm{Im}(z) = -\frac{1}{2}i(z - \overline{z})$.

Beweis. (i) ist offensichtlich. Für (ii) sei $z_1 = a + bi, z_2 = c + di$. Dann ist $z_1 \cdot z_2 = ac - bd + (ad + bc)i$ und

$$\overline{z}_1 \cdot \overline{z}_2 = (a - bi) \cdot (c - di) = ac - bd + (-ad - bc)i = \overline{z_1 \cdot z_2}.$$

(iii) rechnet man entweder von Hand anhand der Formel für das Inverse nach, oder man verwendet die folgende elegantere Methode: Es gilt $z \cdot z^{-1} = 1$. Wir konjugieren alles, und erhalten mit (ii)

$$\overline{z}\overline{z^{-1}} = \overline{z \cdot z^{-1}} = \overline{1} = 1.$$

Also ist $\overline{z^{-1}}$ das (eindeutige) multiplikativ Inverse zu $\overline{z}$. Das ist gerade die Aussage. (iv) und (v) sind klar. Für (vi) setzen wir $z = a + bi$ und rechnen

$$z + \overline{z} = a + bi + a - bi = 2a = 2\mathrm{Re}(z),$$

und das ist gerade die erste Aussage. Weiter ist

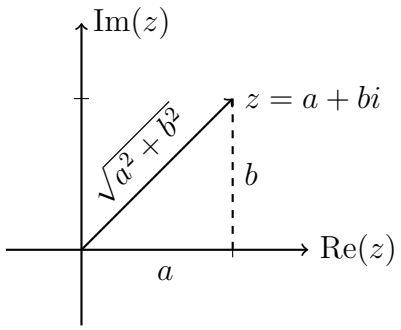
$$z - \overline{z} = a + bi - (a - bi) = 2bi = 2\mathrm{Im}(z)i.$$

Wenn wir mit $-\frac{1}{2}i$ multiplizieren, erhalten wir rechts genau $\mathrm{Im}(z)$, da $i^2 = -1$. □

Eine weitere wichtige Struktur auf $\mathbb{C}$ ist der *Betrag* einer komplexen Zahl. Für $z = a + bi \in \mathbb{C}$ definieren wir ihn als

$$|z| = \sqrt{a^2 + b^2}.$$

Man beachte, dass $a^2 + b^2$ eine positive reelle Zahl ist, aus der wir eine positive reelle Quadratwurzel ziehen können.
Der Betrag $|z|$ ist gerade die Länge von z als Vektor in $\mathbb{R}^2$, wie man mit dem Satz des Pythagoras sieht:



Auch stimmt der Betrag $|a|$ für reelle Zahlen genau mit dem alten Betrag überein, d.h. $|a| = a$ falls $a \geq 0$ und $|a| = -a$ falls $a < 0$.

Satz 1.5.6. *Für $z, z_1, z_2 \in \mathbb{C}$ gilt*

(i) $|z| \in \mathbb{R}, |z| \geq 0$, *und* $|z| = 0 \Leftrightarrow z = 0$

(ii) $|\mathrm{Re}(z)| \leq |z|$ *und* $|\mathrm{Im}(z)| \leq |z|$

(iii) $|\overline{z}| = |z|$.

(iv) $z \cdot \overline{z} = |z|^2$, *und also* $z^{-1} = \frac{1}{|z|^2}\overline{z}$ *für* $z \neq 0$.

(v) $|z_1 \cdot z_2| = |z_1| \cdot |z_2|$

(vi) $|z_1 + z_2| \leq |z_1| + |z_2|$ *(Dreiecksungleichung)*

Beweis. (i) ist klar. Für (ii) sei $z = a + bi$. Es gilt

$$|\mathrm{Re}(z)| = |a| = \sqrt{a^2} \leq \sqrt{a^2 + b^2} = |z|,$$

und analog für $\mathrm{Im}(z) = b$. (iii) ist ebenfalls klar. Für (iv) rechnen wir

$$z \cdot \overline{z} = (a + bi) \cdot (a - bi) = a^2 - b^2 i^2 = a^2 + b^2 = |z|^2.$$

Für (v) verwenden wir (iv) und Satz 1.5.5:

$$|z_1 z_2|^2 = z_1 z_2 \overline{z_1 z_2} = z_1 \overline{z_1} z_2 \overline{z_2} = |z_1|^2 |z_2|^2.$$

Wenn wir auf beiden Seiten die Quadratwurzel ziehen, erhalten wir das Ergebnis. Für (vi) schließlich rechnen wir:

$$\begin{aligned} |z_1 + z_2|^2 &= (z_1 + z_2)\overline{(z_1 + z_2)} = z_1\overline{z}_1 + z_1\overline{z}_2 + z_2\overline{z}_1 + z_2\overline{z}_2 \\ &= |z_1|^2 + |z_2|^2 + z_1\overline{z}_2 + \overline{z_1\overline{z}_2} \\ &= |z_1|^2 + |z_2|^2 + 2\mathrm{Re}(z_1\overline{z}_2). \end{aligned}$$

Dabei haben wir wieder (iv) und Satz 1.5.5 verwendet. Weiter ist

$$\begin{aligned}(|z_1| + |z_2|)^2 &= |z_1|^2 + 2|z_1||z_2| + |z_2|^2 \\ &= |z_1|^2 + 2|z_1 z_2| + |z_2|^2,\end{aligned}$$

wobei wir (v) verwenden. Als Differenz erhalten wir

$$(|z_1| + |z_2|)^2 - |z_1 + z_2|^2 = 2\left(|z_1 z_2| - \mathrm{Re}(z_1\overline{z}_2)\right). \tag{1.25}$$

Da aber

$$|\mathrm{Re}(z_1\overline{z}_2)| \leq |z_1\overline{z}_2| = |z_1||\overline{z}_2| = |z_1||z_2| = |z_1 z_2|$$

nach (ii), (iii) und (v) gilt, ist 1.25 offensichtlich nichtnegativ. Damit gilt

$$|z_1 + z_2|^2 \leq (|z_1| + |z_2|)^2,$$

und nach Ziehen der Quadratwurzel ist das die Dreiecksungleichung. □

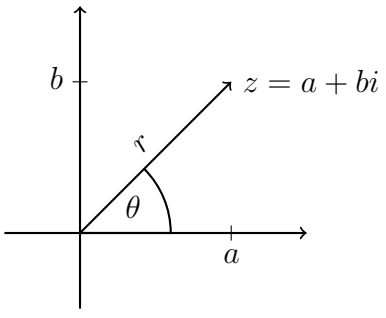
Im folgenden Abschnitt wollen wir die Darstellung komplexer Zahlen in sogenannten *Polarkoordinaten* untersuchen. Wir werden damit eine geometrische Interpretation der Multiplikation erhalten.

1.5.2 Polarkoordinaten

Bisher haben wir komplexe Zahlen z in karthesischen Koordinaten angegeben, d.h. in der Form

$$z = a + bi = (a, b).$$

Man kann die Punkte der Ebene $\mathbb{R}^2$ aber auch in Polarkoordinaten angeben. Jeder Punkt z ist nämlich eindeutig bestimmt durch seinen Winkel θ (von der x-Achse aus gemessen), und seinen Abstand r zum Ursprung.



Dabei ist $\theta \in [0, 2\pi)$ und $r \geq 0$. Die Darstellung

$$z = (r, \theta)$$

nennt man *Polarkoordinatendarstellung* von z. Um Missverständisse zu vermeiden werden wir ab jetzt die karthesischen Koordinaten immer in der Form $z = a + bi$ angeben, und die Tupelschreibweise $z = (r, \theta)$ bleibt den Polarkoordinaten vorbehalten. Wenn nun

$$z = a + bi = (r, \theta),$$

dann gilt offensichtlich

$$r \cdot \sin(\theta) = b, \quad r \cdot \cos(\theta) = a, \quad r^2 = a^2 + b^2 = |z|^2. \tag{1.26}$$

Damit kann man die beiden Darstellungstypen ineinander umrechnen. Sind zum Beispiel die karthesischen Koordinaten a und b gegeben, erhält man

$$r = |z| = \sqrt{a^2 + b^2}, \quad \theta = \arcsin\left(\frac{b}{r}\right) = \arccos\left(\frac{a}{r}\right). \tag{1.27}$$

Sind hingegen die Polarkoordinaten r und θ gegeben, bekommt man direkt

$$a = r \cdot \cos(\theta), \quad b = r \cdot \sin(\theta). \tag{1.28}$$

Beispiel 1.5.7. Sei $z = 1 + i$ in karthesischen Koordinaten gegeben. Wir berechnen $r = |z| = \sqrt{1 + 1} = \sqrt{2}$ sowie

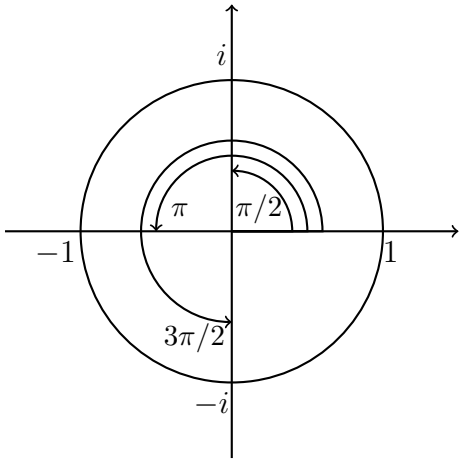
$$\theta = \arcsin\left(\frac{1}{\sqrt{2}}\right) = \pi/4.$$

Also ist

$$z = (\sqrt{2}, \pi/4)$$

die Darstellung in Polarkoordinaten. Für $z_1 = 1, z_2 = i, z_3 = -1, z_4 = -i$ erhält man analog die Polarkoordinaten

$$z_1 = (1, 0),\ z_2 = (1, \pi/2),\ z_3 = (1, \pi),\ z_4 = (1, 3\pi/2).$$



Beispiel 1.5.8. Sei $z = (1, 3\pi/4)$ in Polarkoordinaten gegeben. Wir berechnen die karthesischen Koordinaten:

$$a = 1 \cdot \cos(3\pi/4) = -\frac{1}{\sqrt{2}}, \quad b = 1 \cdot \sin(3\pi/4) = \frac{1}{\sqrt{2}}.$$

Wie schon erwähnt liegt einer der Hauptvorteile der Polarkoordinaten in der besonders schönen Formel für die Multiplikation. Sie erlaubt ein unmittelbares geometrisches Verständis der Multiplikation:

Satz 1.5.9. *Die Multiplikation zweier komplexer Zahlen erfüllt in Polarkoordinaten die folgende Gleichung:*

$$(r, \theta) \cdot (s, \eta) = (r \cdot s, \theta + \eta).$$

Beweis. Sei $z_1 = (r, \theta)$ und $z_2 = (s, \eta)$. Wir rechnen zunächst mit 1.28 in karthesische Koordinaten um:

$$z_1 = r\cos(\theta) + r\sin(\theta)i, \quad z_2 = s\cos(\eta) + s\sin(\eta)i.$$

Nun können wir die Multiplikation durchführen:

$$\begin{aligned} z_1 z_2 = {} & rs\cos(\theta)\cos(\eta) - rs\sin(\theta)\sin(\eta) \\ & + (rs\cos(\theta)\sin(\eta) + rs\sin(\theta)\cos(\eta))\, i. \end{aligned}$$

Es gilt also

$$\mathrm{Re}(z_1 z_2) = rs(\cos(\theta)\cos(\eta) - \sin(\theta)\sin(\eta)) = rs\cos(\theta + \eta)$$

und

$$\mathrm{Im}(z_1 z_2) = rs(\cos(\theta)\sin(\eta) + \sin(\theta)\cos(\eta)) = rs\sin(\theta+\eta).$$

Dabei verwenden wir die als bekannt vorausgesetzten Additionstheoreme für Sinus und Cosinus. Diese Koordinaten rechnen wir nun mit 1.27 wieder in Polarkoordinaten um. Wir erhalten als Betrag von $z_1 z_2$

$$|z_1 z_2| = \sqrt{(rs\cos(\theta+\eta))^2 + (rs\sin(\theta+\eta)^2} = \sqrt{(rs)^2} = rs,$$

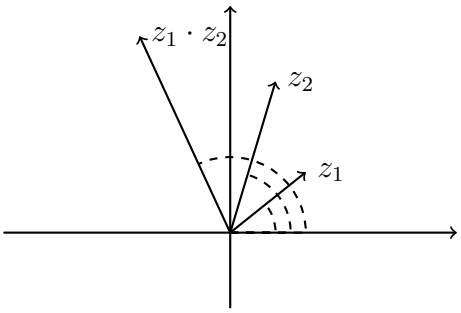
wobei wir $\sin(\varphi)^2 + \cos(\varphi)^2 = 1$ für alle φ verwenden. Für den Winkel von $z_1 z_1$ bekommen wir

$$\arcsin\left(\frac{rs\sin(\theta+\eta)}{rs}\right) = \arcsin(\sin(\theta+\eta)) = \theta+\eta.$$

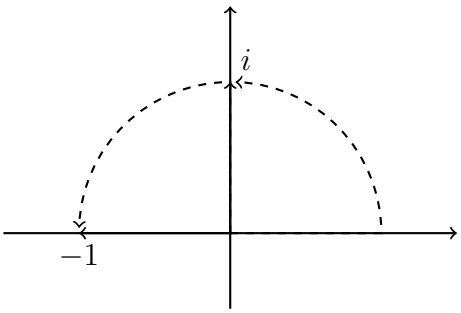
Genau das war zu zeigen. □

Die geometrische Interpretation der Multiplikation ist also einfach:

Man addiert die Winkel der Elemente, und multipliziert ihre Längen.



Auf diese Weise sehen wir auch sofort, warum $i^2 = -1$ gilt:



Im nächsten Abschnitt werden wir jetzt ganz leicht zeigen können, dass man in $\mathbb{C}$ stets beliebige Wurzeln aus allen Elementen ziehen kann.

1.5.3 Wurzeln

In den reellen Zahlen kann man nicht im Allgemeinen beliebige Wurzeln aus Elementen ziehen. Wir haben ja gesehen, dass -1 dort keine Quadratwurzel besitzt, und das war gerade die Motivation zur Konstruktion von $\mathbb{C}$. Aber auch wenn es Wurzeln gibt, gibt es eventuell nicht so viele, wie man vielleicht erwarten könnte. Wenn wir uns beispielsweise für die vierten Wurzeln von 1 interessieren, also für die Lösungen der Gleichung

$$x^4 - 1 = 0,$$

so finden wir in $\mathbb{R}$ gerade 1 und -1. Die Gleichung ist aber gerade vom Grad 4, und wir könnten deshalb ja sogar bis zu 4 verschiedene Lösungen erwarten. In der Tat sind ja i und $-i$ weitere Lösungen der Gleichung, die aber echt komplex sind.

Satz 1.5.10 (Existenz von Einheitswurzeln)**.** *Sei $n \geq 1$ eine positive ganze Zahl. Dann gibt es genau n verschiedene Zahlen $1 = \zeta_0, \zeta_1, \ldots, \zeta_{n-1} \in \mathbb{C}$ mit*

$$\zeta_j^n = 1$$

für alle $j = 0, \ldots, n-1$.

Beweis. Wir geben die ζ_j in Polarkoordinaten an:

$$\zeta_j := (1, 2\pi j/n).$$

Die ζ_j sind offensichtlich paarweise verschieden, da sie die paarweise verschiedenen Winkel

$$0,\ 2\pi/n,\ 4\pi/n,\ 6\pi/n,\ \ldots,\ 2\pi(n-1)/n$$

besitzen. Auch $\zeta_0 = 1$ ist klar. Mit Satz 1.5.9 gilt

$$\zeta_j^n = (1^n, n \cdot 2\pi j/n) = (1, 2\pi j) = 1,$$

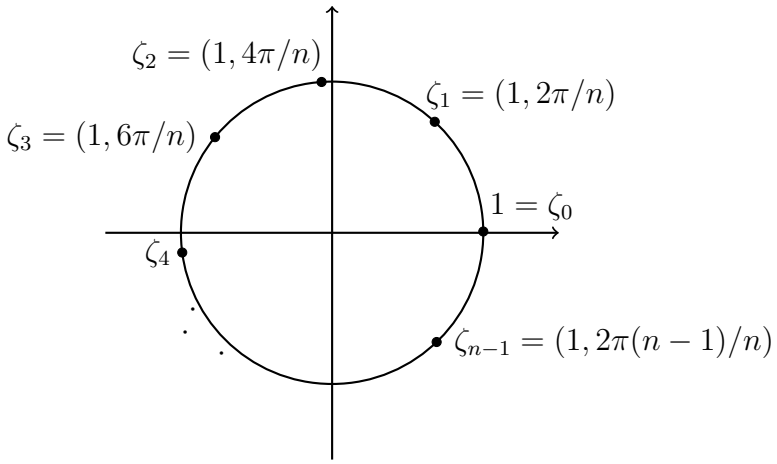
da Vielfache von 2π ja gerade dem Winkel 0 entsprechen.
Es bleibt noch zu zeigen, dass es nicht mehr n-te Wurzeln aus 1 gibt. Falls $\zeta = (r, \varphi)$ mit $r \geq 0$ und $\varphi \in [0, 2\pi)$ aber

$$1 = \zeta^n = (r^n, n\varphi)$$

erfüllt, so muss $r^n = 1$ und $n\varphi = 2\pi j$ für ein $0 \leq j \leq n-1$ gelten. Daraus folgt $r = 1$ und $\varphi = 2\pi j/n$, also $\zeta = \zeta_j$. □

Definition 1.5.11. Die ζ_j aus dem letzten Satz werden auch *n-te Einheitswurzeln* genannt.

Wir erhalten die n-ten Einheitswurzeln also gerade durch die Einteilung des Einheitskreises in $\mathbb{C}$ in n gleiche Stücke:

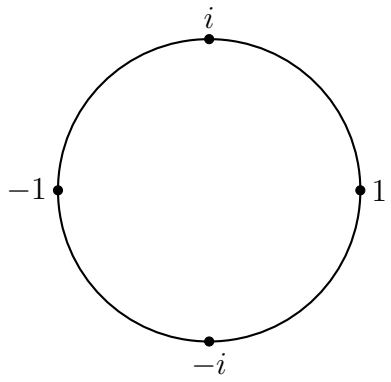


Wenn man also ζ_1 mit sich selbst mutlipliziert, wandert es einen Schritt weiter zu ζ_2. Die dritte Potenz ist ζ_3, usw. In der n-ten Potenz ist man gerade einmal durch den Kreis gelaufen, und bei 1 gelandet.

Wenn man ζ_2 quadriert erhält man ζ_4. Aus der Formel $\zeta_2^n = (1, 4\pi)$ sieht man, dass man nach der n-ten Potenz gerade *zweimal* durch den Kreis gelaufen ist, und bei der 1 landet.

Allgemein wandert ζ_j beim potenzieren j mal durch den Kreis, und landet nach der n-ten Potenz bei 1. Ein ζ_j kann allerdings auch schon vorher einmal 1 ergeben.

Beispiel 1.5.12. Sein $n = 4$. Wir finden die 4-ten Einheitswurzeln $1, i, -1, -i$:



Es gilt

$$1^1 = 1^2 = 1^3 = 1^4 = 1$$

$$i^1 = i,\ i^2 = -1,\ i^3 = -i,\ i^4 = 1$$

$$(-1)^1 = -1,\ (-1)^2 = 1,\ (-1)^3 = -1,\ (-1)^4 = 1$$

$$(-i)^1 = -i,\ (-i)^2 = -1,\ (-i)^3 = i,\ (-i)^4 = 1.$$

Die Zahlen 1 und -1 ergeben also schon in kleinerer Potenz als 4 einmal 1. Sie sind ja auch 2-te Einheitswurzeln. Die Zahlen i und $-i$ werden erst nach dem vierten Potenzieren das erste Mal 1.

Definition 1.5.13. Eine n-te Einheitswurzel, die *das erste Mal* in der n-ten Potenz 1 ergibt, heißt *primitive n-te Einheitswurzel*.

Beispiel 1.5.14. Es sind i und $-i$ primitive 4-te Einheitswurzeln. Die -1 ist keine primitive 4-te Einheitswurzel, aber eine primitive 2-te Einheitswurzel. Die 1 ist eine (die!) primitive erste Einheitswurzel.

Man kann nun sehr einfach auch Wurzeln aus anderen Elementen ziehen:

Satz 1.5.15. *Sei $n \geq 1$ eine positive ganze Zahl und $0 \neq z \in \mathbb{C}$. Dann gibt es genau n verschiedene Zahlen $\omega_1, \ldots, \omega_n \in \mathbb{C}$ mit*

$$\omega_j^n = z$$

für $j = 1, \ldots, n$.

Beweis. Schreibe $z = (r, \varphi)$ in Polarkoordinaten, mit $r > 0$ und $\varphi \in [0, 2\pi)$. Die offensichtlichste n-te Wurzel aus z entsteht, indem man den Winkel durch n teilt und die n-te Wurzel aus dem positiven Radius zieht:

$$\omega_1 = (\sqrt[n]{r}, \varphi/n).$$

Seien nun $1 = \zeta_0, \zeta_1, \ldots, \zeta_{n-1}$ die n-ten Einheitswurzeln. Setze

$$\omega_j = \zeta_{j-1} \cdot \omega_1$$

für $j = 2, \ldots, n$. Wir multiplizieren ω_1 also gerade mit den n-ten Einheitswurzeln. Es entstehen dabei weitere n-te Wurzeln aus z:

$$\omega_j^n = \zeta_{j-1}^n \omega_1^n = 1 \cdot z = z.$$

Die ω_j sind außerdem paarweise verschieden, aufgrund der Kürzungsregel.
Sei nun $\omega = (s, \psi)$ eine weitere n-te Wurzel aus z, mit $s \geq 0$ und $\psi \in [0, 2\pi)$. Es gilt also

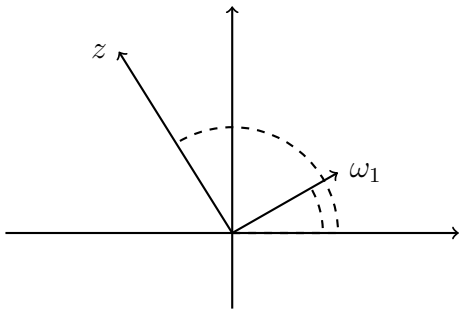
$$(r, \varphi) = z = \omega^n = (s^n, n \cdot \psi),$$

und damit $s = \sqrt[n]{r}$, $\psi = \frac{1}{n}(\varphi + 2\pi j)$ für ein $0 \leq j \leq n-1$. Damit ist

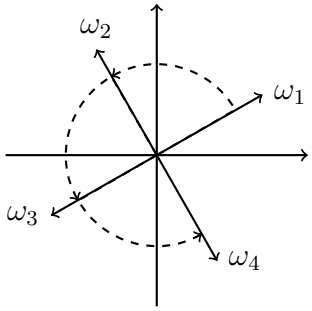
$$\omega = (\sqrt[n]{r}, \varphi/n + 2\pi j/n) = (1, 2\pi j/n) \cdot (\sqrt[n]{r}, \varphi/n) = \zeta_j \cdot \omega_1 = \omega_{j+1}.$$

Also gibt es keine weiteren n-ten Wurzeln außer den ω_j. □

Wir sehen, wie man die Wurzeln geometrisch zu verstehen hat. Die offensichtlichste n-te Wurzel ω_1 aus z entsteht durch Teilung des Winkels durch n und Ziehen der n-ten Wurzel aus dem Radius (hier zum Beispiel $n = 4$):



Die weiteren n-ten Wurzeln aus z entstehen durch Multiplikation von ω_1 mit den ζ_j, also durch Addition der Vielfachen von $2\pi/n$ zum Winkel:



1.5.4 Der Fundamentalsatz der Algebra

Wir haben gesehen, dass sich in $\mathbb{C}$ sehr viele Gleichungen lösen lassen, wie etwa

$$x^n - a = 0,$$

mit $a \in \mathbb{C}$. Der *Fundamentalsatz der Algebra* besagt, dass sich *alle* polynomialen Gleichungen lösen lassen:

Satz 1.5.16 (Fundamentalsatz der Algebra)**.** *Seien $a_0, a_1, \ldots, a_n \in \mathbb{C}$, wobei $n \geq 1$ und $a_n \neq 0$. Dann gibt es ein $z \in \mathbb{C}$ mit*

$$a_0 + a_1 z + a_2 z^2 + \cdots + a_n z^n = 0.$$

Jede polynomiale Gleichung vom Grad $n \geq 1$ besitzt also eine Lösung.

Für den Fundamentalsatz der Algebra gibt es eine Menge verschiedener Beweise aus unterschiedlichen Bereichen der Mathematik. Sie sind aber alle zu umfangreich für den Rahmen der Vorlesung. Wir wollen nur noch einmal erklären, wie der Satz in unseren Kontext einzuordnen ist.
Wir haben mit den ganzen Zahlen $\mathbb{Z}$ begonnnen. Dort waren Gleichungen der Gestalt

$$ax - b = 0$$

teilweise nicht lösbar. Durch Übergang zu den rationalen Zahlen $\mathbb{Q}$ haben wir dieses Problem behoben. Allerdings haben wir gesehen, dass beispielsweise die Gleichung

$$x^2 - 2 = 0$$

keine Lösung in $\mathbb{Q}$ besaß. Durch die Konstruktion von $\mathbb{R}$ wurde dieses Problem wiederum behoben. Hier gab es aber dann noch keine Lösung der Gleichung

$$x^2 + 1 = 0,$$

was uns zur Konstruktion von $\mathbb{C}$ veranlasst hat. Der Fundamentalsatz der Algebra besagt nun, dass wir hier keine weiteren unlösbaren polynomialen Gleichungen finden werden. Der Erweiterungsprozess der Zahlbereiche ist damit in gewisser Weise an ein natürliches Ende gekommen.
Ebenfalls an ein natürliches Ende gekommen ist damit der erste Teil der Vorlesung. Wir haben wichtige Zahlbereiche und Ergebnisse der elementaren Zahlentheorie kennengelernt. Im zweiten Teil wollen wir nun etwas abstraktere Algebra betreiben. Wir werden mit Axiomen anstelle von konkreten Zahlbereichen arbeiten. Viele der Strukturen werden offensichtliche Verallgemeinerungen von bereits Bekanntem sein.

Kapitel 2

Abstrakte Algebra

In diesem Teil der Vorlesung wollen wir etwas abstrakte Algebra kennenlernen. Wir arbeiten mit Axiomen, die aus den Strukturen des letzten Kapitels abgeleitet sind. Wir werden dann Aussagen ausschließlich anhand der Axiome beweisen. Der Vorteil dieser Vorgehensweise ist, dass wir Ergebnisse für große Klassen von Strukturen auf einmal bekommen, und sie nicht in jedem konkreten Fall erneut zeigen müssen. Wir beginnen mit einem der wichtigesten grundlegenden Begriffe der Algebra, dem einer *Gruppe*.

2.1 Gruppen

> *Das entscheidende Kriterium ist Schönheit; für häßliche Mathematik ist auf dieser Welt kein beständiger Platz.*
>
> Godfrey Harold Hardy (1877-1947)

2.1.1 Definition, Beispiele und Eigenschaften

Definition 2.1.1. Eine *Gruppe* ist eine Menge G, zusammen mit einer zweistelligen Verknüfpung

$$*\colon G \times G \to G,$$

welche die folgenden Bedingungen erfüllt:

$$\forall a, b, c: \quad a * (b * c) = (a * b) * c \qquad \text{(Assoziativität)} \tag{2.1}$$

$$\exists e\, \forall a: \quad e * a = a \qquad \text{(Existenz neutrales Element)} \tag{2.2}$$

$$\forall a\, \exists b: \quad b * a = e \qquad \text{(Existenz inverse Elemente)} \tag{2.3}$$

Falls zusätzlich noch die folgende Eigenschaft gilt, nennt man G eine *abelsche* oder *kommutative Gruppe*:

$$\forall a, b: \quad a * b = b * a \qquad \text{(Kommutativgesetz)} \tag{2.4}$$

Bemerkung 2.1.2. (i) Anstelle von $*$ wird die Verknüpfung oft auch mit $+, \cdot$ oder $\circ$ bezeichnet. Auch für das neutrale Element e verwendet man oft andere Bezeichnungen. Falls die Verknüpfung mit $+$ bezeichnet wird, schreibt man oft 0 statt e. Im Falle von $\cdot$ ist 1 statt e die gebräuchliche Bezeichnung. Bei $\circ$ schreibt man manchmal id für das neutrale Element.
(ii) Die Definition der inversen Elemente nimmt bezug auf das neutrale Element. Es wird gefordert, dass $b * a$ das neutrale Element ergibt. Insbeondere muss klar sein, welches Element neutral bezüglich $*$ ist, bevor über inverse Elemente gesprochen werden kann.
(iii) Man beachte, dass in vielen Büchern die Existenz eines Elements gefordert wird, das von *beiden Seiten* neutral ist, d.h. das $e * a = a * e = a$ für alle $a \in G$ erfüllt. Außerdem wird oft gefordert, dass ein *beidseitig* inverses Element zu jedem a existiert. Wir werden jedoch in Satz 2.1.6 zeigen, dass diese Eigenschaften aus unseren bereits folgen. Das linksneutrale Element ist zum Beispiel automatisch auch rechtsneutral, man muss das nicht extra fordern.

Man beachte, dass die Gruppenaxiome gerade den Eigenschaften (1.2), (1.3), (1.4) und für die Kommutativität (1.1) entsprechen. Dort wurde allerdings $+$ als Schreibweise für die Verknüpfung gewählt.
Wir haben im ersten Teil schon viele Gruppen kennengelernt:

Beispiel 2.1.3. (i) Die ganzen Zahlen $\mathbb{Z}$ mit $+$ bilden eine abelsche Gruppe. Das neutrale Element ist die 0.

(ii) Die Restklassenringe $\mathbb{Z}/n\mathbb{Z}$ sind abelsche Gruppen bezüglich $+$. Das neutrale Element ist die Restklasse der Null: $[0]_n$.

(iii) Die rationalen Zahlen $\mathbb{Q}$ bilden eine abelsche Gruppe bezüglich $+$. Genauso sind die reellen Zahlen $\mathbb{R}$ und die komplexen Zahlen $\mathbb{C}$ eine Gruppe bezüglich $+$.

(iv) Die Menge $\mathbb{Q} \setminus \{0\}$ bildet eine abelsche Gruppe bezüglich $\cdot$, mit neutralem Element 1. Jede rationale Zahl ungleich Null ist nämlich multiplikativ invertierbar. Genauso sind $\mathbb{R} \setminus \{0\}$ und $\mathbb{C} \setminus \{0\}$ bezüglich $\cdot$ eine Gruppe mit neutralem Element 1.

(v) Die Menge der positiven reellen Zahlen $\mathbb{R}_{>0}$ ist eine abelsche Gruppe bezüglich $\cdot$. Das Inverse einer positiven Zahl ist ja wieder positiv. Die negativen reellen Zahlen sind keine Gruppe bezüglich $\cdot$, denn die Verknüpfung überführt zwei negative Zahlen in eine positive.

(vi) Falls p eine Primzahl ist, ist $(\mathbb{Z}/p\mathbb{Z}) \setminus \{0\}$ eine Gruppe bezüglich $\cdot$. Das ist gerade die Aussage von Satz 1.2.13

(vii) Falls n keine Primzahl ist, ist $(\mathbb{Z}/n\mathbb{Z}) \setminus \{0\}$ auch keine Gruppe bezüglich $\cdot$. Die Existenz von nicht invertierbaren Elementen folgt zum Beispiel aus Korollar 1.2.11.

(viii) Im Allgemeinen bezeichne $(\mathbb{Z}/n\mathbb{Z})^\times$ die Menge aller Element von $\mathbb{Z}/n\mathbb{Z}$, die ein multiplikativ Inverses besitzen. Es sind gerade die Restklassen von Zahlen, die teilerfremd zu n sind. Dann ist $(\mathbb{Z}/n\mathbb{Z})^\times$ eine Gruppe mit $\cdot$. Im Falle einer Primzahl ist das gerade Beispiel (vi).

(ix) $\mathbb{Z}\setminus\{0\}$ ist *keine* Gruppe bezüglich $\cdot$. Die 2 zum Beispiel besitzt kein inverses Element.

(x) $\mathbb{Q}$ ist keine Gruppe bezüglich $\cdot$. Die Null ist nicht multiplikativ invertierbar. Das gleiche gilt für $\mathbb{R}$ und $\mathbb{C}$.

(xi) Wenn $(G, *, e)$ und $(H, \circ, e')$ Gruppen sind, dann ist das karthesische Produkt

$$G \times H = \{(a, b) \mid a \in G, b \in H\}$$

eine Gruppe mit der Verknüpfung

$$(a, b) \cdot (c, d) := (a * c, b \circ d).$$

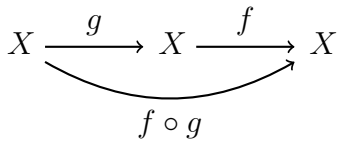
Das neutrale Element ist (e, e'), und wenn a' invers zu a und b' invers zu b ist, ist (a', b') invers zu (a, b).

Alle bisherigen Beispiele waren abelsche Gruppen. Die ersten Beispiele nichtabelscher Gruppen sind die *Permutationsgruppen*.

Beispiel 2.1.4. Sie X eine nichtleere Menge und

$$S(X) = \{f \colon X \to X \mid f \text{ bijektiv }\}$$

die Menge aller bijektiven Selbstabbildungen von X. Eine bijektive Abbildung von X heißt auch *Permutation* (d.h. Vertauschung) von X. Wir versehen $S(X)$ mit der Hintereinanderausführung $\circ$ von Funktionen:



$$(f \circ g)(x) := f(g(x)) \qquad \forall x \in X.$$

Es ist bekannt, dass die Hintereinanderausführung bijektiver Funktionen wieder bijektiv ist, und dass die Hintereinanderausführung von Funktionen dem Assoziativitätsgesetz genügt. Also ist

$$\circ \colon S(X) \times S(X) \to S(X)$$

eine zweistellige assoziative Verknüpfung. Wir bezeichnen die identische Abbildung mit id, d.h.

$$\mathrm{id}(x) = x \quad \forall x \in X.$$

Offensichtlich gilt

$$\mathrm{id} \circ f = f$$

für alle $f \in S(X)$, d.h. id ist neutral bezüglich $\circ$. Schließlich besitzt jede bijektive Funktion f eine Umkehrfunktion $f^{-1} \colon X \to X$, die gerade

$$f^{-1} \circ f = \mathrm{id}$$

erfüllt. Somit ist $S(X)$ eine Gruppe bezüglich $\circ$, mit neutralem Element id . Sie wird *Permutationsgruppe von* X genannt.

Wir wollen uns im folgenden meißt auf endliche Mengen beschränken:

Beispiel 2.1.5. Sei X eine endliche Menge der Mächtigkeit $n \geq 1$. Wir können $X = \{1, \ldots, n\}$ annehmen, und bezeichnen die Permutationsgruppe $S(X)$ dann

auch mit S_n. Wir notieren Permutationen von X wie folgt. In eine Zeile schreiben wir die Zahlen $1, \ldots, n$, und in eine Zeile darunter ihre Bilder unter der Abbildung. So bezeichnet

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}$$

gerade die Abbildung $\sigma\colon \{1,2,3,4\} \to \{1,2,3,4\}$, die 1 auf 3, 2 auf 2, 3 auf 4 und 4 auf 1 abbildet. Das neutrale Element hat also die Darstellung

$$\mathrm{id} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}.$$

Das inverse Element zu einer Permutation erhält man dann gerade durch Vertauschen der beiden Zeilen (und umsortieren der Spalten). So erhält man zum Beispiel

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}$$

als Inverses zu σ von oben.
Möchte man in dieser Schreibweise Permutationen verknüpfen (d.h. hintereinanderausführen), schreibt man sie hintereinander, und liest dann von rechts nach links die Werte ab. So gilt zum Beispiel

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}.$$

Ganz explizit erhält man für $n = 2$

$$S_2 = \left\{ \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\} = \{\mathrm{id}, \tau\}.$$

Dabei gilt $\mathrm{id} \circ \tau = \tau \circ \mathrm{id} = \tau$ und $\tau^2 = \mathrm{id}$. Die Gruppe ist also abelsch, und τ ist sein eigenes multiplikativ Inverses.
Die Gruppe S_3 hat die Elemente

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

Hier rechnet man

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

und

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

Somit ist S_3 *nicht* abelsch!

Wir wollen nun einige einfache Eigenschaften von Gruppen beweisen. Dabei verwenden wir nur die Gruppenaxiome.

Satz 2.1.6. *Sei G eine Gruppe mit Verknüfpung $*$. Dann gilt:*

(i) Das neutrale Element e ist eindeutig bestimmt, d.h. es gibt keine zwei verschiedenen Elemente, die 2.2 erfüllen.

(ii) Es gilt $a * e = a$ für alle $a \in G$.

(iii) Zu jedem $a \in G$ gibt es genau ein $b \in G$ mit $b * a = e$.

(iv) Aus $b * a = e$ folgt auch $a * b = e$.

(v) In G gilt die beidseitige Kürzungsregel, d.h. $a * f = a * g$ sowie $f * a = g * a$ implizieren jeweils $f = g$.

Beweis. Wir beweisen zunächst (iv). Es gelte also $b * a = e$. Sei nun c ein inverses Element zu b, d.h. es gelte $c * b = e$. Die Existenz von c ist durch 2.3 gesichert. Wir rechnen nun

$$\begin{aligned} a * b &= e * (a * b) = (c * b) * (a * b) = c * ((b * a) * b) \\ &= c * (e * b) = c * b = e. \end{aligned}$$

Dabei haben wir mehrfach das Assoziativgesetz und die (Links-)Neutralität von e benutzt. Für (ii) sei b so dass $b * a = e$. Dann ist

$$a * e = a * (b * a) = (a * b) * a = e * a = a.$$

Dabei haben wir (iv) benutzt.
Für (i) sei e' ein weiteres Element, das 2.2 erfüllt. Mit $a = e$ folgt dann

$$e' * e = e.$$

Wenn wir gleichzeitig (ii) mit $a = e'$ verwenden bekommen wir

$$e' * e = e',$$

und zusammengesetzt also $e = e'$.
Wir beweisen nun (v). Sei dazu b invers zu a. Wenn wir die Gleichung $a * f = a * g$ von links mit b multiplizieren erhalten wir $f = g$. Analog können wir die Gleichung $f * a = g * a$ von rechts mit b multiplizieren, wobei wir (iv) und (ii) verwenden.
Die Existenz in (iii) ist schließlich gerade eines der Gruppenaxiome, die Eindeutigkeit folgt aus der Kürzungsregel. □

Man beachte, dass (ii) und (iv) in abelschen Gruppen trivial sind. In nicht-abelschen Gruppen gelten sie aber eben auch.
Die Eindeutigkeit der inversen Elemente erlaubt es uns, sie in Zukunft mit $-a$ oder a^{-1} zu bezeichnen, je nach Notation der Verknüpfung. Bei $+$ wird gewöhnlich $-a$ gewählt, bei $*, \cdot$ und $\circ$ schreibt man a^{-1}.

Lemma 2.1.7. *In einer Gruppe G mit Verknüpfung $*$ gilt für Elemente a, b*

$$(a^{-1})^{-1} = a, \quad (a * b)^{-1} = b^{-1} * a^{-1}.$$

Beweis. Die erste Aussage besagt gerade, dass a das inverse Element zu a^{-1} ist. Das ist aber trivial, da $a * a^{-1} = e$ gilt. Die zweite Aussage besagt, dass $b^{-1} * a^{-1}$ das inverse Element zu $a * b$ ist. Das sieht man wie folgt:

$$(a * b) * (b^{-1} * a^{-1}) = a * ((b * b^{-1}) * a^{-1}) = a * (e * a^{-1}) = a * a^{-1} = e.$$

□

Wir wollen zum Abschluss dieses Abschnittes noch die *Gruppentafel* einer (endlichen) Gruppe erwähnen. Es handelt sich dabei um eine quadratische Matrix, deren Zeilen und Spalten mit den Gruppenelementen indiziert sind. An der Schnittstelle von Zeile a und Spalte b steht dann genau das Produkt $a * b$. Dadurch ist die Gruppenverknüpfung eindeutig bestimmt. Wir geben hier die Gruppentafel für $\mathbb{Z}/3\mathbb{Z}$ mit $+$ an:

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Wenn man die Zeilen und Spalten wie hier in der gleichen Reihenfolge indiziert, übersetzt sich die Kommutativität der Gruppe gerade in die Symmetrie der Matrix (bezüglich Spiegelung an der Diagonalen). Die Existenz von Inversen bedeutet, dass in jeder Zeile und Spalte (genau) einmal das neutrale Element auftaucht.

2.1.2 Homomorphismen und Untergruppen

Wenn man in der Mathematik bestimmte Strukturen betrachtet, interessiert man sich meist auch für Abbildungen zwischen ihnen. Dabei sind oft nur die Abbildungen interessant, die die gegebenen Strukturen erhalten. Im Falle von Gruppen bedeutet das, dass die Abbildungen mit den Verknüpfungen verträglich sein sollten. Das wird durch den Begriff des *Gruppenhomomorphismus* fomalisiert:

Definition 2.1.8. (i) Seien $(G, *, e)$ und $(H, \circ, e')$ Gruppen. Eine Abbildung $\varphi\colon G \to H$ heißt *Gruppenhomomorphismus*, wenn

$$\varphi(a * b) = \varphi(a) \circ \varphi(b)$$

für alle $a, b \in G$ gilt.
(ii) Ein bijektiver Gruppenhomomorphismus heißt *Isomorphismus*.
(iii) Zwei Gruppen heißen *isomorph*, wenn es einen Isomorphismus zwischen ihnen gibt.

Beispiel 2.1.9. Wir haben im ersten Kapitel die Einbettungen von $\mathbb{Z}$ nach $\mathbb{Q}$, von $\mathbb{Q}$ nach $\mathbb{R}$ und von $\mathbb{R}$ nach $\mathbb{C}$ betrachtet. Dabei stellten wir immer fest, dass die neu definierten Verknüpfungen auf der alten Menge mit den dortigen Verknüpfungen übereinstimmten. Die exakte Formulierung dafür ist, dass all diese Einbettungen *Gruppenhomomorphismen* waren.

Beispiel 2.1.10. Die Projektion auf die Restklassen

$$\begin{aligned} \pi\colon \mathbb{Z} &\to \mathbb{Z}/n\mathbb{Z} \\ a &\mapsto [a]_n \end{aligned}$$

ist ein Gruppenhomomorphismus. Da die Verknüpfung auf $\mathbb{Z}/n\mathbb{Z}$ vertreterweise definiert ist gilt

$$\pi(a+b) = [a+b]_n = [a]_n + [b]_n = \pi(a) + \pi(b).$$

Es ist kein Isomorphismus. Da $\mathbb{Z}$ unendlich und $\mathbb{Z}/n\mathbb{Z}$ endlich ist, kann π nicht injektiv sein.

Beispiel 2.1.11. Die Einbettung $\iota\colon \mathbb{Z}/n\mathbb{Z} = \{0, 1, \dots, n-1\} \subset \mathbb{Z}$ ist kein Gruppenhomomorphismus. In $\mathbb{Z}/n\mathbb{Z}$ gilt ja zum Beispiel $1 + (n-1) = 0$. Also müsste

$$0 = \iota(0) = \iota(1 + (n-1)) = \iota(1) + \iota(n-1) = 1 + (n-1) = n$$

in $\mathbb{Z}$ gelten. Das stimmt aber nicht.

Beispiel 2.1.12. Die Multiplikation mit einem festen Element r aus $\mathbb{R}$ ist ein Gruppenhomomorphimus

$$\begin{aligned} m_r\colon \mathbb{R} &\to \mathbb{R} \\ a &\mapsto ra \end{aligned}$$

Es gilt

$$m_r(a+b) = r \cdot (a+b) = ra + rb = m_r(a) + m_r(b).$$

Für $r \neq 0$ ist es sogar ein Isomorphismus. Die Umkehrabbildung ist nämlich $m_{r^{-1}}$.

Beispiel 2.1.13. Die Multiplikation mit einem festen Element $r \neq 0$ ist *kein* Gruppenhomomorphismus von $\mathbb{R} \setminus \{0\}$ nach $\mathbb{R} \setminus \{0\}$, außer für $r = 1$. Es ist gewöhnlich $r \cdot (ab) \neq (ra) \cdot (rb)$.

Beispiel 2.1.14. Die Exponentialabbildung ist ein Gruppenhomomorphismus

$$\begin{aligned} \exp\colon (\mathbb{R}, +, 0) &\to (\mathbb{R}_{>0}, \cdot, 1) \\ a &\mapsto e^a. \end{aligned}$$

Es gilt $\exp(a+b) = e^{a+b} = e^a \cdot e^b = \exp(a) \cdot \exp(b)$. Bekanntermaßen ist $\exp$ bijektiv, also ein Isomorphismus. Somit sind die beiden Gruppen $(\mathbb{R}, +, 0)$ und $(\mathbb{R}_{>0}, \cdot, 1)$ isomorph.

Beispiel 2.1.15. Es gibt einen Isomorphismus $\varphi\colon S_2$ nach $\mathbb{Z}/2\mathbb{Z}$. Schreibt man $S_2 = \{\mathrm{id}, \tau\}$ wie in Beispiel 2.1.5, so definiert $\varphi(\mathrm{id}) = 0, \varphi(\tau) = 1$ einen bijektiven Homomorphismus.

Wir wollen einige leichte Eigenschaften von Gruppenhomomorphismen beweisen.

Lemma 2.1.16. *Sei $\varphi\colon G \to H$ ein Gruppenhomomorphismus. Dann gilt*

$$\varphi(e) = e'$$

und für alle $a \in G$

$$\varphi(a^{-1}) = \varphi(a)^{-1}.$$

Beweis. Es gilt

$$e' \circ \varphi(e) = \varphi(e) = \varphi(e * e) = \varphi(e) \circ \varphi(e).$$

Die erste Behauptung folgt also aus der Kürzungsregel. Zweitens wird gerade behauptet, dass $\varphi(a^{-1})$ das inverse Element zu $\varphi(a)$ in H ist. Wir rechnen also

$$\varphi(a) \circ \varphi(a^{-1}) = \varphi(a * a^{-1}) = \varphi(e) = e'.$$

□

Eine Abbildung ist bekanntlich injektiv, wenn alle Elemente im Zielbereich höchstens ein Urbild haben. Bei Gruppenhomomorphismen reicht es, das Urbild des neutralen Elements zu betrachten:

Lemma 2.1.17. *Ein Gruppenhomomorphismus $\varphi\colon G \to H$ ist genau dann injektiv, wenn gilt*

$$\varphi^{-1}(e') = \{e\}.$$

Beweis. Wie erwähnt bedeutet injektiv, dass alle Urbilder höchstens einelementig sind. Wegen $\varphi(e) = e'$ impliziert die Injektivität also $\varphi^{-1}(e') = \{e\}$. Setzen wir nun umgekehrt diese Bedingung voraus. Sei weiter $\varphi(a) = \varphi(b)$ für gewisse $a, b \in G$. Dann folgt

$$e' = \varphi(a) \circ \varphi(b)^{-1} = \varphi(a) \circ \varphi(b^{-1}) = \varphi(a * b^{-1}).$$

Nach Annahme gilt also $a * b^{-1} = e$, also $a = b$. Somit ist φ injektiv. □

Lemma 2.1.18. *Ist $\varphi\colon G \to H$ ein Isomorphismus, so ist die Umkehrabbildung $\varphi^{-1}\colon H \to G$ automatisch wieder ein Gruppenhomomorphismus.*

Beweis. Übungsaufgabe. □

Bemerkung 2.1.19. Sind zwei Gruppen G und H isomorph, so handelt es sich im wesentlichen um dieselben Gruppen. Sie unterscheiden sich nur durch die Namen der Elemente. Ein Isomorphismus gibt genau diese Umbenennung an. So sind S_2 und $\mathbb{Z}/2\mathbb{Z}$ eigentlich die selben Gruppen. Einmal heißt die Verknüpfung $\circ$, einmal $+$. Das Element $\tau \in S_2$ trägt in $\mathbb{Z}/2\mathbb{Z}$ den Namen 1. Man sieht das nochmal deutlicher, wenn man die Gruppentafeln vergleicht:

$$\left(\begin{array}{c|cc} \circ & \mathrm{id} & \tau \\ \hline \mathrm{id} & \mathrm{id} & \tau \\ \tau & \tau & \mathrm{id} \end{array}\right) \qquad \left(\begin{array}{c|cc} + & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array}\right)$$

Ebenso sind, wenn auch nicht so offensichtlich, auch $(\mathbb{R}, +, 0)$ und $(\mathbb{R}_{>0}, \cdot, 1)$ im Prinzip dieselbe Gruppe. Das Element, das in der ersten Gruppe den Namen a trägt, trägt in der zweiten den Namen e^a. Einmal bezeichnen wir die Verknüpfung mit $+$, einmal mit $\cdot$.

Ein weiterer wichtiger Begriff ist der einer *Untergruppe*.

Definition 2.1.20. Sei G eine Gruppe. Eine nichtleere Teilmenge $U \subseteq G$ heißt *Untergruppe von G*, wenn für alle $a, b \in U$ gilt

$$a * b \in U \quad \text{und} \quad a^{-1} \in U.$$

Bemerkung 2.1.21. Eine Untergruppe enthält immer das neutrale Element e der Gruppe G. Sei nämlich $a \in U$ beliebig. Dann ist $e = a * a^{-1} \in U$. Die Bedingung dass U nichtleer ist, kann also durch die Bedingung $e \in U$ ersetzt werden.

Bemerkung 2.1.22. Dass U eine Untergruppe von G ist bedeutet gerade, dass U mit der von G vererbten Verknüpfung selbst wieder eine Gruppe ist.

Beispiel 2.1.23. In der folgenden Kette sind alle Teilmengen jeweils Untergruppen:

$$\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}.$$

Beispiel 2.1.24. Die Menge $2\mathbb{Z} = \{2a \mid a \in \mathbb{Z}\}$ aller gerade Zahlen ist eine Untergruppe von $\mathbb{Z}$. Die Menge aller ungerade Zahlen ist keine Untergruppe. Sie ist weder abgeschlossen unter $+$, noch enthält sie die 0. Es ist aber allgemeiner für jedes $n \in \mathbb{Z}$ die Menge

$$n\mathbb{Z} = \{n \cdot a \mid a \in \mathbb{Z}\}$$

aller Vielfachen von n eine Untergruppe.

Satz 2.1.25. *Jede Untergruppe von $\mathbb{Z}$ ist von der Gestalt $n\mathbb{Z}$, mit $n \in \mathbb{Z}$.*

Beweis. Sei $U \subseteq \mathbb{Z}$ eine Untergruppe. Der Fall $U = \{0\}$ bedeutet gerade $n = 0$. Im Fall $U \neq \{0\}$ enthält U positive Zahlen. Sei n die kleinste aller positiven Zahlen, die zu U gehören. Aus den Untergruppenaxiomen folgt sofort

$$n\mathbb{Z} \subseteq U.$$

Für die andere Richtung sei $u \in U$ beliebig, aber o.B.d.A. strikt positiv. Also ist $n \leq u$. Wir führen Division mit Rest durch:

$$u = a \cdot n + r$$

mit $0 \leq r < n$. Aus

$$r = u - na$$

und den Untergruppenaxiomen folgt $r \in U$. Weil aber $0 \leq r < n$ und n die kleinste positive Zahl in U war, folgt $r = 0$. Das bedeutet aber $u = an \in n\mathbb{Z}$. □

Lemma 2.1.26. *Sei $\varphi\colon (G, *, e) \to (H, \circ, e')$ ein Gruppenhomomorphismus. Dann ist der Kern von φ*

$$\ker(\varphi) := \{a \in G \mid \varphi(a) = e'\}$$

eine Untergruppe von G, und das Bild von φ

$$\mathrm{im}(\varphi) := \{\varphi(a) \mid a \in G\}$$

ist eine Untergruppe von H.

Beweis. Es gilt $\varphi(e) = e'$, also $e \in \ker(\varphi)$. Seien weiter $a, b \in \ker(\varphi)$. Dann ist

$$\varphi(a * b) = \varphi(a) \circ \varphi(b) = e' \circ e' = e'.$$

Also ist auch $a * b \in \ker(\varphi)$. Schließlich ist $\varphi(a^{-1}) = \varphi(a)^{-1} = e'^{-1} = e'$, und also auch $a^{-1} \in \ker(\varphi)$. Damit ist $\ker(\varphi)$ ist eine Untergruppe.
Es gilt $\varphi(e) = e' \in \mathrm{im}(\varphi)$. Für $a, b \in G$ ist $\varphi(a) \circ \varphi(b) = \varphi(a * b) \in \mathrm{im}(\varphi)$ und $\varphi(a)^{-1} = \varphi(a^{-1}) \in \mathrm{im}(\varphi)$. Also ist $\mathrm{im}(\varphi)$ eine Untergruppe von H. □

Beispiel 2.1.27. Sei $\pi\colon \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ die Projektion aus Beispiel 2.1.10. Dann besteht $\ker(\pi)$ genau aus den Zahlen, die auf $[0]_n$ abgebildet werden, also aus den Vielfachen von n. Es gilt also $\ker(\pi) = n\mathbb{Z}$.

2.1.3 Quotienten

Wir wollen nun noch einmal abstrakt die Konstruktion anschauen, die wir mit $\mathbb{Z}/n\mathbb{Z}$ schon kennengelernt haben. Sei dazu $U \subseteq G$ eine Untergruppe der Gruppe G. Wir definieren eine Äquivalenzrelation $\sim_U$ auf G wie folgt:

$$a \sim_U b :\Leftrightarrow a * b^{-1} \in U.$$

Man beachte, dass in additiver Schreibweise die Bedingung auf der rechten Seite gerade $a - b \in U$ ist. Im Fall $G = \mathbb{Z}$ und $U = n\mathbb{Z}$ ist das genau die Äquivalenzrelation, die wir zur Konstruktion von $\mathbb{Z}/n\mathbb{Z}$ verwendet haben.

Lemma 2.1.28. *Wenn U eine Untergruppe von G ist, ist $\sim_U$ eine Äquivalenzrelation auf G.*

Beweis. Die Reflexivität folgt aus $a * a^{-1} = e \in U$. Die Symmetrie folgt aus der Gleichung

$$b * a^{-1} = (a * b^{-1})^{-1}.$$

Wenn schließlich $a * b^{-1} \in U$ und $b * c^{-1} \in U$, so ist auch

$$a * c^{-1} = (a * b^{-1}) * (b * c^{-1}) \in U.$$

Das beweist die Transitivität. □

Auch im allgemeinen Fall betrachten nun wieder die Äquivalenzklassen von $\sim_U$:

$$[a]_U = \{b \in G \mid b \sim_U a\} = \{b \in G \mid b * a^{-1} \in U\} = a * U.$$

Die Äquivalenzklassen erhält man also gerade, indem man U innerhalb von G von links *verschiebt*. Insbesondere ist U selbst eine Äquivalenzklasse, nämlich

$$U = e * U = [e]_U.$$

Die Äquivalenzklassen werden auch *(Links)-Nebenklassen* oder *Restklassen* von U genannt. Die Menge aller Äquivalenzklassen bezeichnen wir mit G/U:

$$G/U := \{[a]_U \mid a \in G\} = \{a * U \mid a \in G\}.$$

Wir wollen nun ganz analog zu $\mathbb{Z}/n\mathbb{Z}$ die Menge G/U wieder mit einer Gruppenstruktur versehen:

$$[a]_U * [b]_U := [a * b]_U. \tag{2.5}$$

Auch hier ist wieder eine Wohldefiniertheit zu zeigen, denn die Definition von $*$ nimmt Bezug auf Vertreter der Äquivalenzklassen, und die sind nicht eindeutig bestimmt. Es stellt sich heraus, das wir wirklich noch eine *zusätzliche* Forderung an die Untergruppe U stellen müssen, um die Wohldefiniertheit zu bekommen.

Definition 2.1.29. Sei G eine Gruppe, und $U \subseteq G$ eine Untergruppe. U heißt *Normalteiler* von G, falls für alle $a \in G$

$$a * U = U * a$$

gilt. Dabei ist $a * U = \{a * u \mid u \in U\}$ und $U * a = \{u * a \mid u \in U\}$.

Bemerkung 2.1.30. (i) Die Normalteilerbedingung fordert die Gleichheit der *Mengen* $a*U$ und $U*a$. Sie besagt gerade, dass für jedes $u \in U$ ein $v \in U$ existiert mit $a*u = v*a$, und umgekehrt für jedes $v \in U$ ein $u \in U$ existiert mit $v*a = a*u$. Man kann also a an Elementen von U vorbeiziehen, muss das Element allerdings dabei eventuell durch ein anderes Element aus U ersetzen.
(ii) Man die kann Normalteilerbedingung auch so formulieren: ob man U von links oder von rechts um a verschiebt, ist egal. Man sagt auch, dass *Rechts- und Linksnebenklassen übereinstimmen*.
(iii) Falls die Gruppe G kommutativ ist, gilt $a*u = u*a$ für alle $a \in G, u \in U$. Man muss das Element u also beim Vertauschen mit a nicht ersetzen. Das impliziert insbesondere $a*U = U*a$, ist aber im Allgemeinen stärker. Insbesondere ist aber jede Untergruppe einer kommutativen Gruppe automatisch ein Normalteiler.

Beispiel 2.1.31. (i) Die Untergruppe $n\mathbb{Z}$ ist ein Normalteiler von $\mathbb{Z}$, denn $\mathbb{Z}$ ist kommutativ.
(ii) Wir betrachten $G = S_3$, und darin die Untergruppe

$$U = \left\{ \mathrm{id}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \right\}.$$

Wir berechnen

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \circ U = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$$

und

$$U \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \right\}.$$

Diese beiden Mengen stimmen nicht überein, und also ist U kein Normalteiler von S_3.
(iii) Betrachtet man dagegen

$$U = \left\{ \mathrm{id}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\},$$

so stellt man fest, dass U ein Normalteiler von S_3 ist. Dafür rechnet man einfach $\sigma \circ U = U \circ \sigma$ von Hand für alle $\sigma \in S_3$ nach.

Wie angekündigt muss man die Normalteilerbedingung an U stellen, um die Wohldefiniertheit der Verknüpfung auf G/U zu erhalten:

Satz 2.1.32. *Sei U ein Normalteiler der Gruppe G. Dann ist die in 2.5 definierte Verknüpfung auf G/U wohldefiniert. Dadurch wird G/U wieder zu einer Gruppe. Das neutrale Element ist dabei $[e]_U$ und das inverse Element zu $[a]_U$ ist $[a^{-1}]_U$. Falls G abelsch ist, so auch G/U.*

Beweis. Wir beginnen mit der Wohldefiniertheit. Sei also $[a]_U = [a']_U$ und $[b]_U = [b']_U$. Das bedeutet also $a * a'^{-1} \in U$ und $b * b'^{-1} \in U$. Wir müssen

$$[a * b]_U = [a' * b']_U,$$

also $(a * b) * (a' * b')^{-1} = a * b * b'^{-1} * a'^{-1} \in U$ zeigen. Wegen $b * b'^{-1} \in U$ gibt es ein $u \in U$ mit

$$a * b * b'^{-1} = u * a.$$

Hier benützen wir die Gleichheit $a * U = U * a$, also genau die Normalteilereigenschaft von U. Nun ist

$$a * b * b'^{-1} * a'^{-1} = u * a * a'^{-1} \in U,$$

denn $a * a'^{-1} \in U$, und U ist als Untergruppe abgeschlossen unter der Verknüpfung $*$. Damit ist die Wohldefiniertheit gezeigt.
Der Rest ist nun leicht. Die Assoziativität von $*$ auf G/U folgt direkt aus der Assoziativität in G:

$$[a]*([b]*[c]) = [a]*[b*c] = [a*(b*c)] = [(a*b)*c] = [a*b]*[c] = ([a]*[b])*[c].$$

Weiter ist

$$[e] * [a] = [e * a] = [a]$$

für alle $a \in G$, also ist $[e]$ das neutrale Element in G/U. Schließlich ist

$$[a^{-1}] * [a] = [a^{-1} * a] = [e],$$

also sind alle Elemente invertierbar.
Wenn G abelsch ist gilt

$$[a] * [b] = [a * b] = [b * a] = [b] * [a],$$

also ist auch G/U abelsch. □

Definition 2.1.33. Die Gruppe G/U wird *Quotientengruppe, Restklassengruppe* und manchmal *Faktorgruppe von G nach U* genannt.

Beispiel 2.1.34. Die Gruppe $\mathbb{Z}/n\mathbb{Z}$ ist ein explizites Beispiel der abstrakten Konstruktion G/U. Man verwendet $G = \mathbb{Z}$ und $U = n\mathbb{Z}$.

Beispiel 2.1.35. Wie betrachten $G = S_3$ und den Normalteiler

$$U = \left\{ \mathrm{id}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}.$$

Man rechnet nach, dass es genau zwei Nebenklassen von U gibt, und zwar U selbst und

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ U = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\}.$$

Es entsteht also die zweielementige Gruppe

$$S_3/U = \left\{ U, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ U \right\} = \{\mathrm{id}, \tau\}.$$

Es gilt

$$\tau^2 = \left[\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}^2 \right] = [\mathrm{id}] = \mathrm{id}\,.$$

Wir sehen also, das wir gerade wieder die Gruppe S_2 bzw. $\mathbb{Z}/2\mathbb{Z}$ als Quotientengruppe erhalten.

Beispiel 2.1.36. Wir betrachten $G = \mathbb{R}$ und $U = \mathbb{Z}$. U ist Normalteiler von G, denn G ist abelsch. Wir bekommen also die Quotientengruppe

$$\mathbb{R}/\mathbb{Z}.$$

Jede Restklasse von U hat genau einen Vertreter im Intervall $[0, 1)$, denn es sind zwei reelle Zahlen genau dann äquivalent, wenn ihre Differenz ganzzahlig ist. Wir schreiben also etwas salopp

$$\mathbb{R}/\mathbb{Z} = [0, 1).$$

Die Verknüpfung ist analog zu der Verknüpfung in $\mathbb{Z}/n\mathbb{Z}$ zu verstehen. Wir addieren zunächst ganz normal wie in $\mathbb{R}$, und gehen dann wieder zur Restklasse über. Wenn wir das Intervall $[0, 1)$ also nach oben verlassen, treten wir von unten wieder ein. Wir können uns die Gruppe $\mathbb{R}/\mathbb{Z}$ also als einen (kontinuierlichen) Kreis vorstellen.

Lemma 2.1.37. *Sei G eine Gruppe und U ein Normalteiler von G. Dann ist die Projektion*

$$\begin{aligned}\pi\colon G &\to G/U\\ a &\mapsto [a]_U\end{aligned}$$

ein Gruppenhomomorphismus, und es gilt

$$\ker(\pi) = U.$$

Beweis. Für $a, b \in G$ ist

$$\pi(a * b) = [a * b] = [a] * [b] = \pi(a) * \pi(b).$$

Außderdem ist $\pi(e) = [e]$ das neutrale Element in G/U. Also ist π ein Gruppenhomomorphismus. Weiter ist

$$\ker(\pi) = \{a \in G \mid [a] = [e]\} = \{a \in G \mid a \sim_U e\} = \{a \in G \mid a \in U\} = U.$$

□

2.1.4 Der Homomorphiesatz und die Sätze von Lagrange und Fermat

Wir wollen drei interessante und wichtige Sätze der elementare Gruppentheorie beweisen. Der erste ist der *Homomorphiesatz* für Gruppen, der unzählige Anwendungen besitzt.

Satz 2.1.38 (Homomorphiesatz für Gruppen)**.** *Sei $\varphi\colon G \to H$ ein Gruppenhomomorphismus. Dann ist $\ker(\varphi)$ ein Normalteiler von G, und es gibt einen wohldefinierten und injektiven Homomorphismus*

$$\begin{aligned}\overline{\varphi}\colon G/\ker(\varphi) &\to H\\ [a] &\mapsto \varphi(a).\end{aligned}$$

Beweis. Sei $a \in G$ und $u \in \ker(\varphi)$. Es gilt

$$\varphi(a * u * a^{-1}) = \varphi(a) \circ \varphi(u) \circ \varphi(a^{-1}) = \varphi(a) \circ e' \circ \varphi(a)^{-1} = e',$$

also $a*u*a^{-1} \in \ker(\varphi)$. Das bedeutet $a*u = v*a$ für ein $v \in \ker(\varphi)$. Das beweist die Normalteilereigenschaft, und die Gruppe $G/\ker(\varphi)$ ist also wohldefiniert.

Wir zeigen nun die Wohldefiniertheit von $\overline{\varphi}$. Sei dazu $[a] = [b]$, d.h. $a * b^{-1} \in \ker(\varphi)$. Also gilt

$$e' = \varphi(a * b^{-1}) = \varphi(a) \circ \varphi(b)^{-1}.$$

Das impliziert $\varphi(a) = \varphi(b)$, und somit ist $\overline{\varphi}$ wohldefiniert. Die Homomorphieeigenschaft ist dann klar:

$$\overline{\varphi}([a] * [b]) = \overline{\varphi}([a * b]) = \varphi(a * b) = \varphi(a) \circ \varphi(b) = \overline{\varphi}([a]) \circ \overline{\varphi}([b]).$$

Für die Injektivität nutzen wir Lemma 2.1.17. Falls

$$e' = \overline{\varphi}([a]) = \varphi(a)$$

gilt, so ist $a \in \ker(\varphi)$, und damit $[a] = [e]$ in $G/\ker(\varphi)$. Damit ist $\overline{\varphi}$ injektiv. □

Mit dem Homomorphiesatz kann man zum Beispiel die Isomorphie von Gruppen zeigen:

Beispiel 2.1.39. Wir betrachten $S_2 = \{\mathrm{id}, \tau\}$ und den Homomorphismus

$$\begin{aligned} \varphi \colon \mathbb{Z} &\to S_2 \\ n &\mapsto \tau^n \end{aligned}$$

Dabei steht τ^n für das n-fache Produkt $\tau \circ \tau \circ \cdots \circ \tau$ von τ, bzw von τ^{-1}, falls n negativ. Aus $\tau^2 = \mathrm{id}$ folgt $\ker(\varphi) = 2\mathbb{Z}$, und es gibt den injektiven Homomorphismus

$$\begin{aligned} \overline{\varphi} \colon \mathbb{Z}/2\mathbb{Z} &\to S_2 \\ [n] &\mapsto \tau^n \end{aligned}$$

Der Homomorphismus ist offensichtlich auch surjektiv, also ein Isomorphismus.

Der Satz von Lagrange stellt nun eine Beziehung zwischen der Mächtigkeit von G, U und G/U her. Dabei muss U nur eine Untergruppe von G sein, nicht unbedingt Normalteiler. G/U ist dann nur als *Menge* der Äquivalenzklassen von $\sim_U$ zu verstehen, nicht als Gruppe.

Satz 2.1.40 (Satz von Lagrange)**.** *Sei G eine endliche Gruppe, und U eine Untergruppe von G. Dann gilt*

$$|U| \cdot |G/U| = |G|.$$

Insbesondere ist die Mächtigkeit $|U|$ der Untergruppe immer ein Teiler der Gruppenmächtigkeit $|G|$.

Beweis. Die verschiedenen Restklassen $[a] = a * U$ bilden eine disjunkte Zerlegung von G. Das ist bekanntlich für Äquivalenzklassen von Äquivalenzrelationen immer richtig. Es genügt also zu zeigen, dass alle Restklassen dieselbe Mächtigkeit haben. Das ist aber klar, denn

$$a * U = \{a * u \mid u \in U\}$$

besitzt einerseits offensichtlich *höchstens* so viele Elemente wie U, andererseits mindestens so viele. Es folgt ja aus der Kürzungsregel, dass $a * u \neq a * v$ für verschiedene Element $u \neq v$ aus U gilt. □

Beispiel 2.1.41. Wir betrachten die Gruppe S_3. Sie hat 6 Elemente. Also kann sie nur Untergruppen der Mächtigkeit $1, 2, 3$ und 6 besitzen. Die Untergruppen der Mächtigkeit 1 und 6 sind offensichtlich $\{\mathrm{id}\}$ und S_3. Wenn wir also alle weiteren Untergruppen bestimmen wollen, müssen wir nur Teilmengen der Mächtigkeit 2 und 3 untersuchen. Es kann keine Untergruppen mit 4 oder 5 Elementen geben.

Beispiel 2.1.42. Wir betrachen $G = S_3$ und den Normalteiler U aus Beispiel 2.1.35. Aus $|G| = 6$ und $|U| = 3$ folgt sofort $|G/U| = 2$.

Korollar 2.1.43. *Sei G eine endliche Gruppe mit $|G| = p$ prim. Dann besitzt G außer $\{e\}$ und G keine Untergruppen.*

Beweis. Die Mächtigkeit jeder Untergruppe ist ein Teiler von p. Somit kommen nun Mächtigkeit 1 und p in Frage. Das entspricht aber den trivialen Untergruppen $\{e\}$ und G. □

Beispiel 2.1.44. Die Gruppe $\mathbb{Z}/19\mathbb{Z}$ hat nur die beiden trivialen Untergruppen.

Eine schöne Anwendung des Homomorphiesatzes und des Satzes von Lagrange ist das folgende Ergebnis. Es klassifiziert alle endlichen Gruppen mit Primzahlmächtigkeit, und ist eine Verallgemeinerung von Beispiel 2.1.39.

Satz 2.1.45. *Sei G eine endliche Gruppe mit $|G| = p$ prim. Dann gibt es einen Isomorphismus*

$$\mathbb{Z}/p\mathbb{Z} \to G.$$

Insbesondere ist G abelsch.

Beweis. Wir fixieren $a \neq e$ in G und betrachten den Gruppenhomomorphismus

$$\begin{aligned} \varphi\colon \mathbb{Z} &\to G \\ n &\mapsto a^n \end{aligned}$$

Der Kern von φ ist eine Untergruppe, also von der Gestalt $\ker(\varphi) = m\mathbb{Z}$ für ein $m \geq 1$ (G ist endlich!). Es gibt nun einen injektiven Homomorphismus

$$\overline{\varphi}\colon \mathbb{Z}/m\mathbb{Z} \to G.$$

Das Bild $\mathrm{im}(\overline{\varphi})$ ist eine Untergruppe von G (Lemma 2.1.26), die das nichttriviale Element $a = \overline{\varphi}([1])$ enthält. Nach Korollar 2.1.43 bleibt damit aber nur

$$\mathrm{im}(\overline{\varphi}) = G,$$

d.h. $\overline{\varphi}$ ist auch surjektiv. Damit ist es ein Isomorphismus, und es gilt $m = p$. □

Beispiel 2.1.46. Bis auf Isomorphie ist $\mathbb{Z}/19\mathbb{Z}$ die einzige Gruppe mit 19 Elementen.

Beispiel 2.1.47. Wenn n nicht prim ist, kann es nicht-isomorphe Gruppen mit n Elementen geben. So kann es zum Beispiel zwischen

$$\mathbb{Z}/4\mathbb{Z}$$

und

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

keinen Isomorphismus geben. In der letzeren Gruppe gilt für jedes Element $a + a = 0$. In der ersten Gruppe stimmt das nicht. Man überlegt sich, dass es dann keinen Isomorphismus geben kann.

Eine weitere Anwendung ist der folgende Satz:

Satz 2.1.48. *Sei G eine endliche Gruppe und a ein Element aus G. Dann gilt*

$$a^{|G|} = e.$$

Beweis. Wir betrachten wieder den Homomorphismus

$$\begin{aligned} \varphi\colon \mathbb{Z} &\to G \\ n &\mapsto a^n \end{aligned}$$

mit Kern

$$\ker \varphi = m\mathbb{Z},$$

wobei $m \geq 1$. Es gibt den Homomorphismus

$$\overline{\varphi}\colon \mathbb{Z}/m\mathbb{Z} \to G,$$

und es folgt

$$a^m = \overline{\varphi}([m]) = \overline{\varphi}([0]) = a^0 = e.$$

Gleichzeitig ist wegen der Injektivität von $\overline{\varphi}$ das Bild von $\overline{\varphi}$ eine Untergruppe der Mächtigkeit m von G. Aus dem Satz von Lagrange folgt $m||G|$, also $|G| = m \cdot r$ für ein $r \in \mathbb{N}$. Dann ist

$$a^{|G|} = a^{mr} = (a^m)^r = e^r = e.$$

□

Nun können wir leicht den sogannten *kleinen Satz von Fermat* beweisen. Er findet beispielsweise Verwendung in der modernen Kryptografie. Wir erinnern an die Euler'sche φ-Funktion. Es ist $\varphi(n)$ die Anzahl der zu n teilerfremden Zahlen $1 \leq k \leq n$. Außerdem erinnern wir an $(\mathbb{Z}/n\mathbb{Z})^\times$, die Menge aller Elemente von $\mathbb{Z}/n\mathbb{Z}$, die multiplikativ invertierbar sind. Es sind gerade die Restklassen von Zahlen, die teilerfremd zu n sind. Sie bilden eine Gruppe bezüglich $\cdot$ mit genau $\varphi(n)$ Elementen.

Satz 2.1.49 (Kleiner Satz von Fermat)**.** *Es seien a, n teilerfremde ganze Zahlen. Dann gilt*

$$a^{\varphi(n)} \equiv 1 \mod n.$$

Beweis. Wir betrachten das Element $[a] \in \mathbb{Z}/n\mathbb{Z}$, das sogar in $(\mathbb{Z}/n\mathbb{Z})^\times$ liegt, da a und n teilerfremd sind. Wir wenden Satz 2.1.48 in der Gruppe $(\mathbb{Z}/n\mathbb{Z})^\times$ an und erhalten

$$[1] = [a]^{\varphi(n)} = [a^{\varphi(n)}],$$

also $a^{\varphi(n)} \equiv 1 \bmod n$. □

Eine Anwendung des Satzes ist die folgende:

Bemerkung 2.1.50. Seien wieder a und n teilerfremd. Wir wollen eine (hohe) Potenz a^r modulo n berechnen. Wir können nun zuerst r modulo $\varphi(n)$ reduzieren. Falls nämlich $r \equiv s \bmod \varphi(n)$ gilt, also $r = s + k\varphi(n)$, so ist

$$a^r = a^{s+k\varphi(n)} = a^s \cdot (a^{\varphi(n)})^k \equiv a^s \cdot 1^k = a^s \mod n.$$

Beispiel 2.1.51. Wir wollen die letzte Ziffer von

$$7^{999}$$

berechnen. Mit den meisten Standardrechner geht das nicht ohne weiteres. Die letzte Ziffer zu berechnen bedeutet aber gerade, die Zahl modulo 10 zu berechnen. 7 ist teilerfremd zu 10, also können wir wie in der letzten Bemerkung vorgehen. Es ist $\varphi(10) = \varphi(2 \cdot 5) = \varphi(2) \cdot \varphi(5) = 1 \cdot 4 = 4$. Wir dürfen also die Potenz 999 modulo 4 reduzieren. Es ist 996 durch 4 teilbar, also $999 \equiv 3 \bmod 4$. Wir erhalten also

$$7^{999} \equiv 7^3 = 343 \equiv 3 \mod 10.$$

Die letzte Ziffer von 7^{999} ist also eine 3.

Im nächsten Abschnitt wollen wir kurz demonstrieren, wie der kleine Satz von Fermat in der modernen Kryptografie verwendet wird.

2.1.5 Anwendung: Kryptographie

In der Kryptografie untersucht man die Frage, wie Botschaften so verschlüsselt werden können, dass unbefugt mithörende/-lesende Personen den Inhalt der Botschaft nicht verstehen können. Solche Verfahren gibt es seit Tausenden von Jahren. Ursprünglich ersetzte man beipsielsweise jeden Buchstaben des Alphabets durch einen bestimmten anderen. Die Ersetzungsvorschrift musste den teilnehmenden Personen bekannt sein, um die Nachricht wieder zu entschlüsseln. Für andere Personen war die Botschaft aber unverständlich. Natürlich lassen sich so verschlüsselte Nachrichten relativ leicht knacken. Heute verwendet man deshalb sehr viel kompliziertere Methoden. Eine der aktuell gebräuchlichsten ist der *RSA-Algorithmus*. Das besonders interessante daran ist, dass er keine geheime Schlüsselabsprache zwischen den teilnehmenden Personen voraussetzt, und deshalb auch für den Internetverkehr besonders gut geeignet ist.
Jede Person A kann sich zunächst selbst einen *privaten* und einen *öffentlichen* Schlüssel erstellen. Den öffentlichen Schlüssel gibt A öffentlich bekannt, zum Beispiel im Internet. Den privaten Schlüssel hält A geheim. Jede andere Person B kann nun eine Botschaft an A anhand der öffentlichen Schlüssels verschlüsseln. Ist die Botschaft erst einmal verschlüsselt, kann im Idealfall niemand außer A die Botschaft wieder entschlüsseln. B kann die verschlüsselte Botschaft also getrost über unsichere Kanäle wie dem Internet an A schicken, und muss sich vorher auch nie mit A getroffen haben!
Die Methode funktioniert folgendermaßen. Person A wählt sich eine große natürliche Zahl n, und eine weitere Zahl e, die teilerfremd zu $\varphi(n)$ ist. Die Zahlen n und e bilden den öffentlichen Schlüssel, und werden also bekanntgegeben. Den

privaten Schlüssel d berechnet A als das Inverse von e modulo $\varphi(n)$:

$$[d] \cdot [e] = [1] \text{ in } \mathbb{Z}/\varphi(n)\mathbb{Z}.$$

Das geht relativ einfach wenn man $\varphi(n)$ kennt, zum Beispiel mit dem euklidischen Algorithmus.
Person B möchte nun eine Botschaft an A senden. Wir beschränken uns darauf, dass Botschaften Zahlen m mit $m < n$ sind. Ein Text muss eben zunächst anhand einer vereinbarten Methode in solch eine Zahl verwandelt werden (zum Beispiel mit Hilfe des ASCII-Codes). Um die Botschaft zu verschlüsseln berechnet B

$$m^e \mod n.$$

Die Zahlen n und e sind ja bekannt. Das Ergebnis x wird dann an A geschickt. Person A rechnet nun

$$x^d \equiv (m^e)^d = m^{ed} \equiv m^1 = m \mod n.$$

Dabei wird für die dritte Gleichung der kleine Satz von Fermat verwendet, bzw. vielmehr Bemerkung 2.1.50. A hat die Botschaft m also wieder entschlüsselt.
Die Frage ist nun aber, warum niemand sonst diese Entschlüsselung vornehmen kann. Eine Unbefugte Person müsste ja nur ebenfalls den geheimen Schlüssel d kennen. Wir hatten auch gesehen, dass man d anhand der Gleichung $[d] \cdot [e] = [1]$ in $\mathbb{Z}/\varphi(n)\mathbb{Z}$ leicht bekommt, wenn man $\varphi(n)$ kennt. Und n ist ja öffentlich bekannt, deshalb kann man im Prinzip auch $\varphi(n)$ errechnen. Hier kommt jetzt der springende Punkt:

> *Person A muss n so wählen, dass sie selbst $\varphi(n)$ leicht berechnen kann, die Zahl $\varphi(n)$ aber aus der Kenntnis von n allein sehr schwer zu berechnen ist.*

Und das geht folgendermaßen. Person A wählt in Wirklichkeit zwei große Primzahlen p und q, und setzt $n = pq$. Dann gilt nämlich

$$\varphi(n) = \varphi(p \cdot q) = \varphi(p) \cdot \varphi(q) = (p-1)(q-1).$$

Da A ja nicht nur n, sondern auch p und q kennt, geht das sehr einfach. Eine andere Person sieht aber nur n. Die Zahl $\varphi(n)$ kann sie im Prinzip nur dann berechnen, wenn auch sie die Primzahlzerlegung $n = pq$ kennt.

> *Primzahlzerlegung von großen Zahlen ist aber sehr schwer!*

Einzig auf dieser Tatsache beruht die Sicherheit des RSA-Algorithmus. Wir wollen das Ganze in einem sehr einfachen Beispiel illustrieren.

Beispiel 2.1.52. Person A wählt $p = 3$ und $q = 7$. Sie errechnet $n = pq = 21$ und

$$\varphi(21) = \varphi(3)\varphi(7) = 2 \cdot 6 = 12.$$

Dann wählt A noch die Zahl $e = 5$, die teilerfremd zu 12 ist. Die Zahlen

$$(n, e) = (21, 5)$$

bilden den öffentlichen Schlüssel. Der private Schlüssel wird mit dem Euklidischen Algorithmus durch die Gleichung

$$[d] \cdot [5] = [1] \text{ in } \mathbb{Z}/12\mathbb{Z}$$

bestimmt, hier also $d = 5$.
Person B möchte nun die Nachricht $m = 9$ an A senden. Sie rechnet

$$m^e = 9^e = 9^5 = 59049 \equiv 18 \mod 21,$$

und schickt die verschlüsselte Nachricht

$$x = 18.$$

Person A rechnet dann

$$x^d = 18^5 = 1889568 \equiv 9 = m \mod 21,$$

und hat also die Nachricht $m = 9$ entschlüsselt. Ein unbefugter Zuhörer kennt $n = 21, e = 5$ und $x = 18$. Er kann die Botschaft entschlüsseln, wenn er $\varphi(n)$ und damit d kennt. Das ist bei $n = 21$ nicht sehr schwer zu berechnen, da die Primfaktorzerlegung $n = 3 \cdot 7$ einfach zu erhalten ist. Bei sehr viel größeren Primzahlen p und q ist es hingegen selbst mit sehr schnellen Computern nicht zu schaffen.

2.2 Ringe und Körper

Kein Mensch lernt denken, indem er die fertig geschriebenen Gedanken anderer liest, sondern dadurch, daß er selbst denkt.

Mihail Eminescu (1850 - 1889)

2.2.1 Definition, Eigenschaften und Beispiele

Eine Gruppe ist eine Menge mit *einer* Verknüpfung, wie wir im letzten Abschnitt gesehen haben. Im ersten Kapitel der Vorlesung haben wir aber viele Strukturen kennengelernt, in denen es gleichzeitig *zwei* Verknüpfungen, gewöhnlich mit $+$ und $\cdot$ bezeichnet, gibt. Beispiele sind $\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$. Das wird durch den Begriffen *Ring* und *Körper* formalisiert:

Definition 2.2.1. Ein *Ring* ist eine Menge R mit zwei Verknüpfungen

$$+ \colon R \times R \to R \qquad \cdot \colon R \times R \to R,$$

so dass die Axiome (1.1) bis (1.8) aus dem ersten Kapitel gelten.

Bemerkung 2.2.2. (i) Dass R ein Ring ist bedeutet also gerade, dass R mit $+$ eine abelsche Gruppe bildet, die Verknüpfung $\cdot$ assoziativ und kommutativ ist, ein neutrales Element besitzt, und dass das Distributivgesetz gilt.
(ii) Wir wissen dass das neutrale Element bezüglich $+$ eindeutig bestimmt ist. Das stimmt ja in allen Gruppen. Aber auch das neutrale Element bezüglich $\cdot$ ist eindeutig bestimmt. Falls nämlich $1'$ ein weiteres neutrales Element ist, gilt

$$1' = 1 \cdot 1' = 1.$$

(iii) Das neutrale Element von $+$ in einem Ring wird mit 0, das neutrale Element von $\cdot$ mit 1 bezeichnet.
(iv) Die inversen Elemente bezüglich $+$ sind eindeutig bestimmt. Wir bezeichnen das inverse Element zu a mit $-a$.
(v) Multiplikativ inverse Elemente muss es nicht geben. Falls ein Element aber doch eins besitzt, ist es eindeutig bestimmt. Wir bezeichnen es dann mit a^{-1}.
(vi) Man beachte, dass in vielen Büchern die Kommutativität von $\cdot$ in Ringen nicht gefordert wird (vergleiche Beispiel 2.2.3 (v) unten). Falls $\cdot$ doch kommutativ ist, nennt man R dann einen *kommutativen Ring*. In unserer Vorlesung wollen wir die Kommutativität für Ringe aber immer voraussetzen, da viele Beweise und Definitionen sonst deutlich technischer werden.

Beispiel 2.2.3. (i) Das Standardbeispiel für einen Ring ist $\mathbb{Z}$.

(ii) Ebenso sind $\mathbb{Q}, \mathbb{R}$ und $\mathbb{C}$ Ringe.

(iii) $\mathbb{Z}/n\mathbb{Z}$ ist ein Ring für alle $n \in \mathbb{Z}$.

(iv) Die *Gauß'schen Zahlen* $\mathbb{Z}[i]$ sind die Menge aller komplexen Zahlen, deren Real- und Imaginärteil ganze Zahlen sind:

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}.$$

Mit der gewöhnlichen Addition und Multiplikation von komplexen Zahlen ist das ein Ring.

(v) Es bezeichne $\mathrm{M}_d(\mathbb{R})$ die Menge aller $d \times d$-Matrizen mit Einträgen aus $\mathbb{R}$. Man addiert Matrizen einträgeweise, und mulitipliziert sie mit der aus der Linearen Algebra bekannten Matrizenmultiplikation. Dann erfüllt $\mathrm{M}_d(\mathbb{R})$ alle Axiome bis auf die Kommutativität der Multiplikation:

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

In unserem Sinne ist es also kein Ring. Man kann die Kommutativität von $\cdot$ aber auch aus der Axiomenliste streichen. Wir wollen das nicht tun.

(vi) Wenn R und S Ringe sind, ist das karthesische Produkt $R \times S$ mit den komponentenweisen definierten Verknüpfungen wieder ein Ring.

Definition 2.2.4. Ein *Körper* ist eine Menge K mit zwei Verknüpfungen

$$+ \colon K \times K \to K \qquad \cdot \colon K \times K \to K,$$

so dass gilt

(i) K ist mit $+$ eine abelsche Gruppe mit neutralem Element 0

(ii) $K \setminus \{0\}$ ist bezüglich $\cdot$ eine abelsche Gruppe

(iii) Es gilt das Distributivgesetz.

Bemerkung 2.2.5. Ein Körper ist also gerade ein Ring, in dem jedes Element außer der 0 multiplikativ invertierbar ist!

Beispiel 2.2.6. (i) $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sind Körper.

(ii) $\mathbb{Z}/n\mathbb{Z}$ ist genau dann ein Körper, wenn n eine Primzahl ist. Es gibt also auch endliche Körper.

(iii) $\mathbb{Z}$ ist kein Körper.

Lemma 2.2.7. *Sei R ein Ring. Dann gilt*

(i) $0 \cdot a = 0$ *für alle* $a \in R$.

(ii) $(-1) \cdot (-1) = 1$.

(iii) $(-1) \cdot a = -a$ *für alle* $a \in R$.

Beweis. (i) und (ii) genau wie in Lemma 1.1.2 und Lemma 1.1.3. Für (iii) müssen wir zeigen, dass $(-1) \cdot a$ additiv invers zu a ist. Also rechnen wir

$$(-1) \cdot a + a = (-1) \cdot a + 1 \cdot a = (-1 + 1) \cdot a = 0 \cdot a = 0.$$

□

Lemma 2.2.8. *Körper sind nullteilerfrei, d.h.* $a \cdot b = 0$ *impliziert* $a = 0$ *oder* $b = 0$. *Außerdem gilt die Kürzungsregel für* $\cdot$.

Beweis. Es gelte $a \cdot b = 0$ und $a \neq 0$. Durch Multiplikation mit dem Inversen von a erhalten wir

$$b = a^{-1} \cdot 0 = 0.$$

Die Kürzungsregel für $\cdot$ folgt aus der Nullteilerfreiheit wie in Lemma 1.1.4. □

Beispiel 2.2.9. Ringe sind im allgemeinen nicht nullteilerfrei. Wir haben das schon für $\mathbb{Z}/n\mathbb{Z}$ gesehen, wenn n nicht prim ist. Auch die Kürzungsregel für $\cdot$ gilt in Ringen im Allgemeinen nicht.

2.2.2 Homomorphismen, Ideale und Quotienten

Auch bei Ringen (und damit insbesondere auch Körpern) interessieren wir uns für strukturerhaltende Abbildung, genannt *Ringhomomorphismen*.

Definition 2.2.10. (i) Ein *Ringhomomorphismus* ist eine Abbildung $\varphi\colon R \to S$ zwischen Ringen, so das gilt

$$\varphi(0) = 0, \quad \varphi(a + b) = \varphi(a) + \varphi(b)$$

$$\varphi(1) = 1, \quad \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b).$$

(ii) Ein bijektiver Ringhomomorphismus heißt *Isomorphismus* von Ringen.
(iii) Zwei Ringe heißen isomorph, wenn es einen Ringisomorphismus zwischen ihnen gibt.

Bemerkung 2.2.11. (i) Ein Ringhomomorphismus ist insbesondere ein Homomorphismus der Gruppen $(R, +)$ und $(S, +)$. Alle für Gruppenhomomorphismen getroffenen Aussagen gelten also auch hier. So ist beispielsweise ein Ringhomomorphismus genau dann injektiv, wenn der Kern

$$\ker(\varphi) = \{a \in R \mid \varphi(a) = 0\}$$

nur aus der 0 besteht.
(ii) Die Umkehrfunktion φ^{-1} eines bijektiven Ringhomomorphismus ist automatisch wieder ein Ringhomomorphismus.

Beispiel 2.2.12. (i) Die Projektion

$$\begin{aligned} \pi \colon \mathbb{Z} &\to \mathbb{Z}/n\mathbb{Z} \\ a &\mapsto [a] \end{aligned}$$

ist ein Ringhomomorphismus. Die Muliplikation in $\mathbb{Z}/n\mathbb{Z}$ ist ja gerade vertreterweise definiert.

(ii) Die Einbettungen von $\mathbb{Z}$ nach $\mathbb{Q}$ nach $\mathbb{R}$ nach $\mathbb{C}$ sind Ringhomomorphismen.

(iii) Die Multiplikation auf $\mathbb{Z}$ oder $\mathbb{R}$ mit einem festen Element r ist *kein* Ringhomomorphismus, außer für $r = 1$. Die 1 wird ja auf r abgebildet.

Auch für Ringe wollen wir wieder Quotientenstrukturen betrachten. Um die Menge der Restklassen mit einer Ringstruktur versehen zu können, brauchen wir den Begriff eines *Ideals*. Es ist in gewisser Weise ein Analogon zu Normalteilern für Gruppen.

Definition 2.2.13. Eine nichtleere Teilmenge $I \subseteq R$ eines Rings heißt *Ideal*, falls gilt:

$$a, b \in I \Rightarrow a + b \in I$$

und

$$a \in R, b \in I \Rightarrow a \cdot b \in I.$$

Beispiel 2.2.14. In jedem Ring R sind $\{0\}$ und R Ideale. Sie heißen *triviale Ideale*.

Bemerkung 2.2.15. Jedes Ideal enthält die Null, und mit a auch $-a$. Sei nämlich $a \in I$, dann ist

$$0 = 0 \cdot a \in I \text{ und } -a = (-1) \cdot a \in I,$$

wobei wir die zweite Idealeigenschaft und Lemma 2.2.7 verwenden. Also ist I eine Untergruppe von $(R, +)$, und somit ein Normalteiler, da $+$ kommutativ ist.

Beispiel 2.2.16. Für $n \in \mathbb{Z}$ ist $n\mathbb{Z}$ ein Ideal in $\mathbb{Z}$. Nur die zweite Idealeigenschaft ist noch zu zeigen. Es gilt aber für $a, b \in \mathbb{Z}$

$$a \cdot (n \cdot b) = n \cdot (a \cdot b) \in n\mathbb{Z}.$$

Korollar 2.2.17. *Die Ideale von $\mathbb{Z}$ sind genau die Teilmengen $n\mathbb{Z}$.*

Beweis. Wir haben gerade gesehen, dass alle $n\mathbb{Z}$ Ideale sind. Jedes Ideal ist aber insbesondere eine Untergruppe von $(\mathbb{Z}, +)$, und damit gibt es wegen Satz 2.1.25 keine weiteren Ideale. □

Bemerkung 2.2.18. In Körpern K gibt es grundsätzlich nur die beiden trivialen Ideale $\{0\}$ und K. Sei nämlich $I \neq \{0\}$ ein Ideal und $0 \neq a \in I$. Dann gilt

$$I \ni a^{-1} \cdot a = 1,$$

und weiter für alle $b \in K$

$$b = b \cdot 1 \in I.$$

Somit ist $I = K$. Insbesondere ist etwa $\mathbb{Z}$ kein Ideal in $\mathbb{Q}$.

Wir können nun für Ideale I von R einen Quotientenring R/I konstruieren. Dabei gehen wir wie folgt vor. Als *Gruppe* mit $+$ ist R/I definiert wie früher. Die Äquivalenzrelation benutzt also $+$, und ist gerade

$$a \sim_I b : \Leftrightarrow a - b \in I.$$

Da I ja inbesondere ein Normalteiler der Gruppe $(R, +)$ ist, liefert uns das eine Gruppe R/I. Wir versehen nun zusätzlich R/I mit der vertreterweise Multiplikation:

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

Satz 2.2.19. *Wenn I ein Ideal von R ist, ist die vertreterweise Multiplikation wohldefiniert auf R/I. Dadurch wird R/I zu einem Ring mit multiplikativ neutralem Element $[1]$. Die Projektion*

$$\begin{aligned} \pi\colon R &\to R/I \\ a &\mapsto [a] \end{aligned}$$

ist ein Ringhomomorphismus mit $\ker(\pi) = I$.

Beweis. Für die Wohldefiniertheit gelte $[a] = [a']$ und $[b] = [b']$, also $a - a' \in I, b - b' \in I$. Wir müssen $[a \cdot b] = [a' \cdot b']$, also

$$a \cdot b - a' \cdot b' \in I$$

zeigen. Aus $a - a'$ und der zweiten Idealeigenschaft folgt

$$(a - a') \cdot b = ab - a'b \in I.$$

Analog folgt aus $b - b' \in I$

$$a'(b - b') = a'b - a'b' \in I.$$

Die Summe beider Terme auf der rechten Seite liegt wieder in I, und ist gerade $ab - a'b'$. Das zeigt die Wohldefiniertheit.
Da beide Verknüpfungen vertreterweise definiert sind, folgen die Ringeigenschaften direkt aus denen in R. Auch ist pi deshalb ein Ringhomomorphismus, und $\ker(\pi) = I$ folgt bereits aus dem entsprechenden Satz für Gruppen. □

Beispiel 2.2.20. $\mathbb{Z}/n\mathbb{Z}$ ist gerade ein Beispiel für die Quotientenkonstruktion. Es ist also ein Ring, und nicht nur eine Gruppe, wie wir auch schon früher von Hand gezeigt haben.

Beispiel 2.2.21. Die Gruppe $\mathbb{R}/\mathbb{Z} = [0, 1)$ lässt sich *nicht* vertreterweise mit einer Multiplikation versehen. $\mathbb{Z}$ ist auch kein Ideal in $\mathbb{R}$. Explizit wäre etwa

$$\left[\frac{1}{4}\right] = \left[\frac{1}{2} \cdot \frac{1}{2}\right] = \left[\frac{1}{2}\right] \cdot \left[\frac{1}{2}\right] = \left[\frac{3}{2}\right] \cdot \left[\frac{1}{2}\right] = \left[\frac{3}{2} \cdot \frac{1}{2}\right] = \left[\frac{3}{4}\right],$$

was nicht stimmt.

Es gibt nun auch den Homomorphiesatz für Ringe:

Satz 2.2.22 (Homomorphiesatz für Ringe)**.** *Sei $\varphi\colon R \to S$ ein Ringhomomorphismus. Dann ist*

$$\ker(\varphi) = \{a \in R \mid \varphi(a) = 0\}$$

ein Ideal in R, und es gibt einen wohldefinierten und injektiven Ringhomomorphismus

$$\begin{aligned}\overline{\varphi}\colon R/\ker(\varphi) &\to S\\ [a] &\mapsto \varphi(a).\end{aligned}$$

Beweis. Jeder Ringhomomorphismus ist ein Gruppenhomomorphismus der additiven Gruppen. Damit ist $\overline{\varphi}$ ein wohldefinierter injektiver Homomorphismus der additiven Gruppen.
Für $b \in \ker(\varphi)$ und $a \in R$ ist

$$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b) = \varphi(a) \cdot 0 = 0,$$

also auch $a \cdot b \in \ker(\varphi)$. Der Kern ist also ein Ideal.
Es bleibt noch die Ringhomomorphismuseigenschaft von $\overline{\varphi}$ zu zeigen. Die ist auch auch wieder klar:

$$\overline{\varphi}([1]) = \varphi(1) = 1$$

und

$$\overline{\varphi}([a] \cdot [b]) = \overline{\varphi}([a \cdot b]) = \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b) = \overline{\varphi}([a]) \cdot \overline{\varphi}([b]).$$

□

Satz 2.2.23. *Seien n, m zwei positive teilerfremde ganze Zahlen. Dann gilt*

$$\mathbb{Z}/nm\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

als Ringe.

Beweis. Wir betrachten den Ringhomomorphismus

$$\begin{aligned}\pi\colon \mathbb{Z} &\to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}\\ a &\mapsto ([a]_n, [a]_m)\,.\end{aligned}$$

Der Chinesische Restsatz besagt gerade, dass π surjektiv ist. Der Kern von π besteht nun aus den ganzen Zahlen, die von n und m geteilt werden. Aus der Teilerfremdheit folgt

$$\ker(\pi) = nm\mathbb{Z}.$$

Damit erhalten wir einen injektiven (und immer noch surjektiven) Ringhomomorphismus

$$\overline{\pi}\colon \mathbb{Z}/nm\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

Die Ringe sind also isomorph. □

Bemerkung 2.2.24. Wenn n und m nicht teilerfremd sind, erhält man keinen Ringisomorphismus zwischen $\mathbb{Z}/mn\mathbb{Z}$ und $\mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/m\mathbb{Z}$. Wir haben uns schon für $n = m = 2$ in Beispiel 2.1.47 überlegt, dass die beiden Ringe noch nicht mal als additive Gruppen isomorph sind.

Wir können nun endlich Teil (iii) von Satz 1.1.33 zeigen, also die Multiplikativität der Euler'schen φ-Funktion für teilerfremde Zahlen.

Satz 2.2.25. *Seien n, m zwei positive teilerfremde Zahlen. Dann gilt für die Euler'sche φ-Funktion:*

$$\varphi(nm) = \varphi(n) \cdot \varphi(m).$$

Beweis. Wir wissen nach Satz 2.2.23 dass die Ringe $\mathbb{Z}/nm\mathbb{Z}$ und $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ isomorph sind. In isomorphen Ringen gibt es aber immer gleich viele multiplikativ invertierbare Elemente, wie man sich leicht überlegt. In $\mathbb{Z}/nm\mathbb{Z}$ gibt es aber $\varphi(nm)$ invertierbare Elemente. In $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ ist ein Tupel genau dann invertierbar, wenn beide Einträge invertierbar sind. Somit gibt es dort $\varphi(n) \cdot \varphi(m)$ invertierbare Elemente. □

2.2.3 Polynomringe

Eine wichtige Klasse von Ringen sind die *Polynomringe*. Sei dazu zunächst R ein beliebiger Ring. Ein *Polynom mit Koeffizienten in R* ist ein Ausruck

$$a_0 + a_1 x + a_2 x^2 + \cdots + a_d x^d, \tag{2.6}$$

mit $d \in \mathbb{N}$ und $a_0, a_1, \ldots, a_d \in R$. Die a_i sind die *Koeffizienten* des Polynoms, und x ist eine sogenannte *Unbestimmte* oder *Variable*. Falls $a_d \neq 0$, ist d der *Grad* des Polynoms. Er wird mit $\deg$ bezeichnet. Man setzt

$$\deg(0) = -\infty.$$

Die Menge aller Polynome mit Koeffizienten aus R wird mit $R[x]$ bezeichnet:

$$R[x] = \left\{ a_0 + a_1 x + \cdots + a_d x^d \mid d \in \mathbb{N}, a_i \in R \right\}.$$

Die Menge $R[x]$ kann man mit einer Ringstruktur versehen. Dafür addiert man Polynome *koeffizientenweise*:

$$\left(\sum_{i=0}^{d} a_i x^i\right) + \left(\sum_{j=0}^{d'} b_j x^j\right) := \left(\sum_{i=0}^{\max(d,d')} (a_i + b_i) x^i\right).$$

Also zum Beispiel

$$(1 + x - 2x^2) + (x - 5x^4) = 1 + 2x - 2x^2 - 5x^4.$$

Die Multiplikation wird so ausgeführt, dass das Distributivgesetz gilt, und zusätzlich

$$x^i \cdot x^j = x^{i+j}. \tag{2.7}$$

Man multipliziert ein Produkt also einfach aus, und verwendet 2.7. Ein Beispiel ist

$$(1+x)\cdot(1-x^3) = 1\cdot 1 + 1\cdot(-x^3) + x\cdot 1 + x\cdot(-x^3) = 1 - x^3 + x - x^4 = 1 + x - x^3 - x^4.$$

Die allgemeine Formel für die Multiplikation lautet

$$\left(\sum_{i=0}^{d} a_i x^i\right) \cdot \left(\sum_{j=0}^{d'} b_j x^j\right) = \sum_{k=0}^{d+d'} \left(\sum_{i+j=k} a_i \cdot b_j\right) x^k.$$

Die Gruppenstruktur von $(R[x], +)$ folgt unmittelbar aus der von $(R, +)$. Das Polynom $p = 1$ ist offensichtlich neutral bezüglich $\cdot$, und die Kommutativität von $\cdot$ ist ebenso klar. Assoziativ- und Distributivgesetz rechnet man ohne allzu große Probleme nach. Also ist $R[x]$ ein Ring, genannt der *Polynomring über* R.

Beispiel 2.2.26. Da R als beliebiger Ring zugelassen ist, kann man die Konstruktion auch iterieren. Man startet zum Beispiel mit $\mathbb{R}$ und bildet $R_1 = \mathbb{R}[x]$. Nun bildet man den Polynomring über R_1, wobei man die Unbestimmte nun y nennt, und erhält

$$R_2 = R_1[y] = (\mathbb{R}[x])[y],$$

wobei für diesen Ring die Notation $\mathbb{R}[x, y]$ üblich ist. Auf diese Weise erhält man Polynomringe in beliebig vielen Variablen.

Bemerkung 2.2.27. Jedes Polynom $p \in R[x]$ induziert eine Abbildung

$$p\colon R \to R,$$

indem man ein Element $a \in R$ einfach für die Variable x einsetzt und das Ergebnis berechnet:

$$p(a) = a_0 + a_1 a + a_2 a^2 + \cdots + a_d a^d \in R.$$

Man darf das Polynom selbst aber nicht mit dieser Abbildung verwechseln. Man kann beispielsweise in $(\mathbb{Z}/2\mathbb{Z})[x]$ das Polynom

$$p = x^2 + x$$

betrachten. Es ist offensichtlich nicht das Nullelement in $R[x]$, denn nicht alle Koeffizienten sind Null. Als Abbildung erhält man jedoch

$$p(0) = 0^2 + 0 = 0 \text{ und } p(1) = 1^2 + 1 = 1 + 1 = 2 = 0,$$

also die Nullabbildung auf $\mathbb{Z}/2\mathbb{Z}$. p induziert also die gleiche Abbildung wie das konstante Nullpolynom 0. Als Polynome sind die beiden aber nicht identisch.

Lemma 2.2.28. *Falls R nullteilerfrei ist, so auch $R[x]$. Es gilt also die Kürzungsregel.*

Beweis. Beim Multiplizieren zweier Polynome $f = f_0 + f_1 x + \cdots + f_d x^d$ und $g = g_0 + g_1 x + \cdots + g_{d'} x^{d'}$ ist der Koeffizient von $x^{d+d'}$ gerade $f_d g_{d'}$. Wenn f_d und g_d nicht null sind, ist es das Produkt also auch nicht. □

Im Falle eines Polynomrings in *einer* Variablen über einem *Körper* K hat der Ring $K[x]$ besondere Eigenschaften. Man kann beispielsweise Division mit Rest durchführen, auch als *Polynomdivision* bekannt:

Division mit Rest für Polynome. *Sei K ein Körper, und $f, g \in K[x]$ mit $g \neq 0$ und $\deg(g) \leq \deg(f)$. Dann gibt es Polynome $h, r \in K[x]$ mit*

$$f = h \cdot g + r$$

und $\deg(r) < \deg(g)$.

Beweis. Wir machen Induktion über den Grad von f. Im Fall $\deg(f) = 0$ liegen f und g in K, und die Aussage ist gerade

$$f = (fg^{-1}) \cdot g + 0.$$

Wir schreiben nun

$$f = f_0 + f_1 x + \cdots + f_d x^d, \quad g = g_0 + g_1 x + \cdots + g_e x^e$$

mit $f_d, g_e \neq 0$ und also $e \leq d$. Wir betrachten nun das Polynom

$$r_1 := f - f_d \cdot g_e^{-1} \cdot x^{d-e} \cdot g.$$

Man beachte, dass wir die Invertierbarkeit von g_e verwenden! Es gilt

$$\deg(r_1) < \deg(f),$$

da sich der Leitterm $f_d x^d$ gerade aufhebt. Falls sogar $\deg(r_1) < \deg(g)$ gilt, sind wir fertig:

$$f = f_d \cdot g_e^{-1} \cdot x^{d-e} \cdot g + r_1. \tag{2.8}$$

Ansonsten können wir die Induktionsvoraussetzung auf r_1 und g anwenden:

$$r_1 = h \cdot g + r$$

mit $\deg(r) < \deg(g)$. Wenn wir das aber in 2.8 einsetzen, erhalten wir eine gewünschte Gleichung. □

Beispiel 2.2.29. Wir betrachten $f = x^3 + x + 1$ und $g = 2x^2 - x - 1$ in $\mathbb{Q}[x]$. Im ersten Schritt bilden wir

$$r_1 = f - \frac{1}{2} \cdot x \cdot g = x^3 + x + 1 - x^3 + \frac{1}{2}x^2 + \frac{1}{2}x = \frac{1}{2}x^2 + \frac{3}{2}x + 1.$$

Es gilt $\deg(r_1) \geq \deg(g)$, und wir müssen noch einen Schritt durchführen:

$$r_2 = r_1 - \frac{1}{4}g = \frac{1}{2}x^2 + \frac{3}{2}x + 1 - \frac{1}{2}x^2 + \frac{1}{4}x + \frac{1}{4} = \frac{7}{4}x + \frac{5}{4}.$$

Nun gilt $\deg(r_2) < \deg(g)$, und wir erhalten

$$r_1 = \frac{1}{4}g + r_2$$

sowie

$$f = \frac{1}{2}xg + r_1 = \frac{1}{2}xg + \frac{1}{4}g + r_2 = \left(\frac{1}{2}x + \frac{1}{4}\right) g + r_2.$$

Das ist die gewünschte Gleichung. Oft führt man dieselbe Rechnung auch auf die aus der Schule bekannte Weise als Polynomdivision in einem einzigen Tableau durch.

Eine leichte Folgerung ist die Tatsache, dass man einen *Linearfaktor* abspalten kann, wenn ein Polynom eine Nullstelle hat:

Korollar 2.2.30. *Sei K ein Körper und $f \in K[x]$. Dann gilt $f(a) = 0$ für ein $a \in K$ genau dann wenn*

$$f = h \cdot (x - a)$$

für ein $h \in K[x]$.

Beweis. Aus $f = h \cdot (x-a)$ folgt offensichtlich $f(a) = 0$. Sei umgekehrt $f(a) = 0$. Wir führen Division mit Rest durch:

$$f = h \cdot (x - a) + r$$

mit $\deg(r) < \deg(x-a) = 1$, also $r \in K$. Wenn wir auf beiden Seiten a einsetzen sehen wir aber $r = 0$. □

Korollar 2.2.31. *Sei K ein Körper. Dann hat ein Polynom $0 \neq f \in K[x]$ höchstens $\deg(f)$ viele verschiedene Nullstellen in K.*

Beweis. Wenn f die Nullstelle $a \in K$ hat, können wir $f = h \cdot (x - a)$ schreiben. Von a verschiedene Nullstellen müssen dann Nullstellen von h sein, wegen der Nullteilerfreiheit von K. Man kann also iterativ Linearfaktoren abspalten:

$$f = g \cdot (x - a_1) \cdots (x - a_n),$$

wenn $a_1, \ldots, a_n$ die verschiedenen Nullstellen von f in K sind. Wir haben im Beweis von Lemma 2.2.28 gesehen, dass sich die Grade beim Multiplizieren addieren. Also gilt $n \leq \deg(f)$. □

Das folgende Korollar zeigt, dass das Phänomen aus Bemerkung 2.2.27 über unendlichen Körpern nicht auftritt.

Korollar 2.2.32. *Falls K ein unendlicher Köper ist, und $f \neq g$ zwei unterschiedliche Polynome, so sind auch die induzierten Abbildungen $f\colon K \to K$ und $g\colon K \to K$ unterschiedlich.*

Beweis. Sind f und g als Abbildung auf K gleich, so ist $f - g$ die Nullabbildung auf K. Das Polynom $f - g$ hat also alle Elemente von K als Nullstelle, und das sind unendlich viele. Aus Korollar 2.2.31 folgt $f - g = 0$ in $K[x]$, also $f = g$ als Polynome. □

Im ersten Kapitel haben wir die Division mit Rest für den Euklidischen Algorithmus verwendet. Genau das selbe können wir hier nun auch tun.

Euklidischer Algorithmus für Polynome. *(i) Der Algorithmus erhält als Eingabe zwei Polynome $f, g \in K[x], g \neq 0$, mit $\deg(g) \leq \deg(f)$.*

(ii) Es wird Division mit Rest auf f und g angewandt:

$$f = hg + r$$

mit $\deg(r) < \deg(g)$.

(iii) Falls $r = 0$, so wird g als Ergebnis ausgegeben. Falls $r \neq 0$ so wird Schritt (ii) wiederholt, diesmal mit g anstelle von f und r anstelle von g.

Beispiel 2.2.33. Wir führen den Euklidischen Algorithmus für $f = x^3 + x^2$ und $g = x^2 - 1$ in $\mathbb{Q}[x]$ durch. Im ersten Schritt erhalten wir

$$f = (x + 1) \cdot g + (x + 1).$$

Der zweite Schritt ist

$$g = (x - 1) \cdot (x + 1) + 0.$$

Der Algorithmus liefert also $x + 1$ als Ergebnis.

Satz 2.2.34. *Der Euklidische Algorithmus für Polynome endet nach endlich vielen Schritten. Das Ergebnis ist ein Polynom p mit den folgenden Eigenschaften:*

(i) p teilt sowohl f als auch g.

(ii) Falls ein weiteres Polynom h sowohl f als auch g teilt, so teilt h auch p.

Beweis. Da der Grad von r in jedem Schritt echt sinkt, muss der Algorithmus nach endlich vielen Schritten enden. Der Rest des Beweises geht praktisch wörtlich gleich wie für den Euklidischen Algorithmus in $\mathbb{Z}$. □

Zwei Polynome $f, g \in K[x]$ haben also immer einen größten gemeinsamen Teiler $\mathrm{ggT}(f, g)$. Definiert ist er über die beiden Eigenschaften (i) und (ii) im letzten Satz. Um ihn eindeutig zu machen fordert man oft dass er *normiert* ist, also 1 als Leitkoeffizient hat:

$$p = p_0 + p_1 x + \cdots + x^r.$$

Sehr viele der Aussagen aus $\mathbb{Z}$ gelten auch in $K[x]$, zum Beispiel die eindeutige Primfaktorzerlegung von Elementen. Wir wollen noch die folgende Aussage beweisen (vergleiche mit Korollar 2.2.17):

Satz 2.2.35. *Sei K ein Körper. Dann sind die einzigen Ideale im Ring $K[x]$ von der Gestalt*

$$f \cdot K[x] = \{f \cdot g \mid g \in K[x]\},$$

mit $f \in K[x]$.

Beweis. Zunächst sind die Mengen $f \cdot K[x]$ offensichtlich alles Ideale in $K[x]$. Sei nun I ein beliebiges Ideal in $K[x]$. Falls $I = \{0\}$, so ist $I = 0 \cdot K[x]$. Ansonsten wählen wir unter allen Polynomen $p \in I \setminus \{0\}$, eins von kleinstem Grad, und nennen es f. Dann ist

$$f \cdot K[x] \subseteq I$$

klar. Für die andere Inklusion sei $0 \neq p \in I$ beliebig. Wegen $\deg(f) \leq \deg(p)$ können wir Division mit Rest durchführen:

$$p = h \cdot f + r,$$

mit $\deg(r) < \deg(f)$. Wegen $r = p - hf$ liegt r in I, und aus der Minimilität des Grades von f folgt also $r = 0$. Also ist

$$p = h \cdot f \in f \cdot K[x].$$

Das beweist die andere Inklusion. □

Beispiel 2.2.36. Wir betrachten den Ringhomomorphismus

$$\begin{aligned} \varphi \colon \mathbb{R}[x] &\to \mathbb{C} \\ p &\mapsto p(i). \end{aligned}$$

Er ist offensichtlich surjektiv. Der Kern ist ein Ideal, welches $x^2 + 1$ enthält, aber offensichtlich kein Polynom vom Grad 1. Der letzte Beweis zeigt also dass

$$\ker(\varphi) = (x^2 + 1) \cdot \mathbb{R}[x]$$

gilt. Der Homomorphisatz für Ringe liefert nun einen Isomorphismus

$$\mathbb{R}[x]/(x^2 + 1) \cdot \mathbb{R}[x] \to \mathbb{C}.$$

Das ist eigentlich auch nicht verwunderlich. In dem Quotienten

$$\mathbb{R}[x]/(x^2 + 1) \cdot \mathbb{R}[x]$$

gilt ja

$$0 = [x^2 + 1] = [x]^2 + [1] = [x]^2 + 1.$$

Wir haben also einen Ring der $\mathbb{R}$ enthält, und zusätzlich eine Quadratwurzel aus -1. Genauso haben wir auch $\mathbb{C}$ konstruiert.

Ich bin immer noch verwirrt, aber auf einem höheren Niveau.

Enrico Fermi (1901-1954)