Algebraische Strukturen Teil 1

Anwendung von Abbildungen: Hashing

Hashfunktionen

Abbildungen, die Datensätzen beliebiger Länge (viele Bit) **Hashwerte** fester, meist kürzerer Länge (z.B. 128 Bit) zuordnen.
Dies sind dann Speicheradressen, welche effizientes Suchen von Datensätzen in großen Datenmengen ermöglichen.

Beispiel Hashing

Aufgabe: Finde schnell die Vorwahl von einem beliebigen Ort in Österreich.
Schlüssel (key): Suchbegriff ist in unserem Fall der Ort, mithilfe dessen die Speicheradresse berechnet wird.
Wert (value): gesuchter Wert ist in unserem Fall die Vorwahl.
Idee: Nachdem wir die Speicheradresse mithilfe des Schlüssels berechnen, ist der Zugriff über den Suchbegriff möglich. Wir müssen also nicht mehr die gesamte Datenmenge durchsuchen, sondern können nur die Werte betrachten, welche an der berechneten Speicheradresse zu finden sind.

Die Hashfunktion

Die **Speicheradresse**, die mit Hilfe des Suchbegriffes (sprich Schlüssel k) berechnet wird, wird mittels Hashfunktion (H) ermittelt, welche k als Argument erhält.
Der Schlüssel wird also unter der Adresse H(k) abgelegt und kann auch damit wiedergefunden werden.

$$H : K \to A = \{0, 1, 2, ..., N-1\}$$
$$k \mapsto H(k)$$

Beispiel Hashfunktion

Die Hashfunktion:

$$H(k) = \sum_i a_i \mod N \tag{1}$$

a_i = die Zahl für die Stelle des i-ten Buchstaben z.B. k= XYZ würde bedeuten $a_1 = 24$, $a_2 = 25$, $a_3 = 26$.
$N = 7$. Wir berechnen den Wert für die Schlüssel WIEN, GRAZ, SALZBURG und DORNBIRN.
Wir erhalten:
$H(WIEN) = (23 + 9 + 5 + 14) \mod 7 = 2$
$H(GRAZ) = ?$
$H(SALZBURG) = ?$
$H(DORNBIRN) = ?$
Welche Adressen würden für GRAZ, SALZBURG und DORNBIRN mit der gegebenen Hashfunktion berechnet?

Beispiel Hashfunktion

Die Hashfunktion:

$$H(k) = \sum_i a_i \mod N$$

a_i = die Zahl für die Stelle des i-ten Buchstaben z.B. k= XYZ würde bedeuten $a_1 = 24$, $a_2 = 25$, $a_3 = 26$.
$N = 7$. Wir berechnen den Wert für die Schlüssel WIEN, GRAZ, SALZBURG und DORNBIRN.
Wir erhalten:

$H(WIEN) = (23 + 9 + 5 + 14) \mod 7 = 2$
$H(GRAZ) = (7 + 18 + 1 + 26) \mod 7 = 3$
$H(SALZBURG) = (19 + 1 + 12 + 26 + 2 + 21 + 18 + 7) \mod 7 = 1$
$H(DORNBIRN) = (4 + 15 + 18 + 14 + 2 + 9 + 18 + 14) \mod 7 = 3$

Kollision

Wir sehen, dass wir ein Problem haben, da sowohl Dornbirn als auch Graz **demselben Speicherplatz zugeordnet** werden, ein Sachverhalt, der Kollision genannt wird.
Normalerweise gibt es sehr viele Schlüssel, die auf eine kleinere Anzahl verfügbarer Hashwerte (sprich Speicheradressen) mittels H(k) abgebildet werden sollen.

Kollision

Eine einfache Strategie zur Auflösung von Kollisionen ist das **lineare Sondieren**. Dabei wird die nächst größere freie Adresse gewählt.

$$s_i(k) = \big(H(k) + i\big) \mod N, \text{für } i = 1, \cdots, N-1.$$

Hashtabelle

Eine **Hashtabelle** ist eine Datenstruktur, in der die (key, value)- Paare an der mit der Hashfunktion berechneten Adresse abgespeichert werden.
Wir vermeiden die Kollision zwischen GRAZ und DORNBIRN, indem wir DORNBIRN an der Adresse $(3+1) \mod 7 = 4$ abspeichern.

Speicherplatz(n)	Schluessel(k_n)	Wert(v_n)
0		
1	SALZBURG	0662
2	WIEN	01
3	GRAZ	0316
4	DORNBIRN	05572
5		
6		

Quadratisches Sondieren

Bessere Strategie zur Auflösung von Kollisionen:

$$\left.\begin{array}{rcll} s_{2i-1}(k) & = & \left(H(k)+i^2\right) & \mod N \\ s_{2i}(k) & = & \left(H(k)-i^2\right) & \mod N \end{array}\right\} i = 1, \cdots, \frac{N-1}{2}.$$

d.h. für $N = 7$ gilt:
$H(k)+1, H(k)-1, H(k)+4, H(k)-4, H(k)+9, H(k)-9$

Quadratisches Sondieren. Wie gut funktioniert es?

i	1		2		3	
i^2	1		4		9	
$\pm i^2 \bmod 7$	1	6	4	3	2	5

i	1		2	
i^2	1		4	
$\pm i^2 \bmod 5$	1	4	4	1

Abbildung: Adressen für verschiedenes N.

Beachte: Der Modulo Operator bildet positive Reste, d.h. $-1 = (-1) \cdot 7 + 6$.

siehe Blatt 2

Satz von Fermat (1607-1665)

Ist N eine Primzahl und es gilt $N \mod 4 = 3$, so gilt

$$\{\pm i^2 \mod N : i = 1, \cdots, \tfrac{N-1}{2}\} = \{1, 2, \cdots, N-1\}.$$

Wähle N gemäß dieser Vorschrift, damit eine gleichmäßige Auslastung der Hashtabelle auch im Fall von Kollisionen gewährleistet ist.

Algebraische Strukturen

Algebraische Strukturen:

- Gruppen
- Ringe
- Körper
- Vektorräume (nächste Vorlesung)

Außerdem:

- Teilbarkeit
- und der Algorithmus von Euklid, einer der ältesten Algorithmen überhaupt.

Algebraische Strukturen

Algebraische Strukturen:

Um was gehts hier?

Algebraische Strukturen

Eine algebraische Struktur ist schlicht eine **Menge**, auf der man eine oder mehrere **Operationen** ausführen kann.

Operation bedeutet **Verknüpfungen von Elementen**, also etwa Addition und Multiplikation.

Eine **Operation** ist eine **Abbildung** vom kartesischen Produkt der zugrunde liegenden Menge in die Menge.

Beispiel

Wenn wir z.B. 2+3 berechnen, dann ist das das Ausführen einer Operation auf zwei Gruppenelementen, zumindest wenn die Menge $\mathbb{Z}$ ist und die Addition so definiert ist, wie wir sie kennen.

Algebraische Strukturen

- Gruppen
- Ringe
- Körper
- Vektorräume

unterscheiden sich in den **Eigenschaften der Operationen** die auf der jeweiligen Struktur definiert sind.

Gruppen

Gruppen

Definition:
Eine **Gruppe** G besteht aus einer Menge G und einer Abbildung (Verknüpfung) $* : G \times G \to G$ mit den folgenden Eigenschaften:

(G1) Es gibt ein Element $e \in G$ mit der Eigenschaft $e * a = a * e = a$ für alle $a \in G$.
e heißt **neutrales Element** in G.

(G2) Zu jedem $a \in G$ gibt es ein eindeutig bestimmtes Element $a^{-1} \in G$ mit der Eigenschaft $a * a^{-1} = a^{-1} * a = e$.
a^{-1} heißt **inverses Element** zu a.

(G3) Für alle $a, b, c \in G$ gilt $a * (b * c) = (a * b) * c$.
G ist **assoziativ**.

Gruppen

Definition:
Die Gruppe $(G, *)$ heißt **kommutative Gruppe** oder **abelsche Gruppe**, wenn zusätzlich gilt:

(G4) Für alle $a, b \in G$ gilt $a * b = b * a$.

Gruppen

Beispiele:
$(\mathbb{R}, +)$ ist eine kommutative Gruppe mit neutralem Element $e = 0$ und inversem Element $a^{-1} = -a$.

Überprüfen wir die Eigenschaften:
(G1): $\forall a \in \mathbb{R}$ gilt natürlich $a + 0 = 0 + a = a$.
(G2): Ebenfalls wissen wir, dass $a + (-a) = (-a) + a = 0$ ist.
(G3): Auch $(a + b) + c = a + (b + c)$ akzeptieren wir sofort.

(G4): Wir behaupten, dass $(\mathbb{R}, +)$ kommutativ ist, d.h $a + b = b + a$ gilt. Auch das sehen wir ein.

Hier ist der „Beweis“ quasi trivial, aber oft ist es etwas schwieriger.

Gruppen

Beispiele:
Ist $(\mathbb{R}^-, \cdot)$ eine Gruppe?

Überprüfen wir die Eigenschaften:
(G1) Gibt es in $\mathbb{R}^-$ ein neutrales Element bzgl. der Multiplikation? Wir wissen, dass das neutrale Element bzgl. Multiplikation 1 sein muss. Aber das neutrale Element muss selbst in G sein ($e \in G$), $1 \notin \mathbb{R}^-$, d.h $(\mathbb{R}^-, \cdot)$ kann keine Gruppe sein.

Die Multiplikation ist keine Abbildung von $\mathbb{R}^- \times \mathbb{R}^- \to \mathbb{R}^-$, da z.B. $(-1) \cdot (-1) = 1 \notin \mathbb{R}^-$. Man sagt auch: Die Menge ist nicht **abgeschlossen** ist bzgl. der Verknüpfung. Auch daher keine Gruppe.

Gruppen

Satz:
Sei $(G, *)$ eine Gruppe, dann gilt für alle Elemente $a, b \in G$:

(a) Für das Inverse von $(a * b)$ gilt $(a * b)^{-1} = b^{-1} * a^{-1}$

(b) Das Inverse eines Elements a ist eindeutig.

Beweis:
(a) zu zeigen: $(a * b)$ verknüpft mit seinem Inversen ergibt das neutrale Element, d.h. $(a * b) * (b^{-1} * a^{-1}) = e$
$(a * b) * (b^{-1} * a^{-1}) =$ /wenn wir das Assoziativgesetz (G3) anwenden ergibt sich:
$a * (b * b^{-1}) * a^{-1} =$ /G2: inverses Element
$a * e * a^{-1} =$ /G2: inverses Elt.
$a * a^{-1} = e$ /G1: neutrales Elt.

Beachten Sie: $(a * b)^{-1} = a^{-1} * b^{-1}$ gilt nur in abelschen Gruppen.

Gruppen

Beweis von (b)

(b) zu zeigen: Sei a^{-1} und $\hat{a}$ Inverses zu a, dann gilt: $a^{-1} = \hat{a}$

$a^{-1} = a^{-1} * e$ //G1: Neutrales Element

$= a^{-1} * a * \hat{a}$ //G2: Inverses Element

$= (a^{-1} * a) * \hat{a}$ //G3: Assoziativgesetz

$= e * \hat{a} = \hat{a}$ //G1: Neutrales Element.

Gruppen

Satz/Definition:
Sei $U \subseteq G$ und $(G, *)$ eine Gruppe, dann ist $(U, *)$ eine Gruppe, wenn gilt:

$$a, b \in U \Rightarrow a * b \in U, a^{-1} \in U$$

U heißt dann **Untergruppe** von G.

Beweis:
$*$ ist eine Verknüpfung auf U, da ja $U \subseteq G$ und $*$ Verknüpfung auf G.

(G1) Es ist a und $a^{-1} \in U$, also auch $a * a^{-1} = e$. D.h $e \in G$

(G2) $a^{-1} \in U$ steckt schon in der Forderung.

(G3) $a * (b * c) = (a * b) * c$ stimmt für alle Elemente in G, also auch für $a, b, c \in U \subseteq G$, da für $a, b \in U$ gilt $a * b \in U$, folgt dass
$a * (b * c) = (a * b) * c$ für alle $a, b, c \in U$ hält.

Gruppen

Beispiel

Wir haben gezeigt, dass $(\mathbb{R}, +)$ eine Gruppe ist. Wir behaupten nun, dass $(\mathbb{Z}, +)$ eine Untergruppe davon ist.

- $\mathbb{Z} \subseteq \mathbb{R}$ ist klar.
- $a + b \in \mathbb{Z}$ für alle $a, b \in \mathbb{Z}$ ist glaubwürdig.
- Für $a \in \mathbb{Z}$ gilt, dass das inverse Element $-a$ ist, und das ist ebenfalls in $\mathbb{Z}$.

Blatt 2

Permutationsgruppen

Die bisherigen Beispiele sind eher trivial, da wir noch keinen interessanten Gruppen kennengelernt haben.

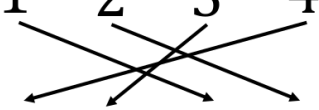
$\Rightarrow$ Permutationsgruppen

Weiß jeder was Permutationen sind?

Notation von Permutationen

Nehmen wir an wir haben eine Menge von Objekten $\{1, 2, 3, 4\}$ auf die wir eine Permutation ausführen. Die Elemente der Menge sind ursprünglich in einer bestimmten Reihenfolge angeordnet. Als Ergebnis der Permutation sind sie anders angeordnet.

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



Alternativ schreiben wir auch oft $\pi = (1\ 3\ 2\ 4)$. Man kann dies lesen als „1 geht in 3 über, 3 in 2, 2 in 4 und 4 in 1“. 1 nimmt also den Platz von 3 ein.

Verkettung von Permutationen

Diese Schreibweise ist auch einfacher, wenn wir Permutationen nacheinander ausführen:

Wir haben $\pi_1 = (1\ 3\ 2)$ und $\pi_2 = (2\ 1\ 3)$ als Permutationen, die wir nacheinander ausführen wollen, also $(1\ 3\ 2) \circ (2\ 1\ 3)$.
Wichtig: Hier wird zuerst (2 1 3) ausgeführt und danach erst (1 3 2).

$(1\ 3\ 2) \circ (2\ 1\ 3)$ d.h. $1 \to 3 \& 3 \to 2$, also $1 \to 2$
$2 \to 1 \& 1 \to 3$, also $2 \to 3$
$3 \to 2 \& 2 \to 1$, also $3 \to 1$

$\Rightarrow (1\ 3\ 2) \circ (2\ 1\ 3) = (1\ 2\ 3)$

Permutationsgruppen

Wir haben gesehen, dass man Permutationen miteinander verknüpfen kann

$S_n \ldots$ Die Menge der Permutationen, die sich auf n Elemente auswirken
Frage: Ist S_n eine Gruppe?

(G1) Neutrales Element ist die Identität, also diejenige Permutation, die nichts verändert:
$\pi(a, b, \ldots, n) = (a, b, \ldots, n)$, also $\pi(i) = i$ für alle i

(G2) Inverses Element muss dasjenige sein, dass alles wieder auf seinen ursprünglichen Platz zurückbringt, also wenn gilt
$\pi(a) = b$, dann $\pi^{-1}(b) = a$

(G3) Assoziativität: $\pi_1 \circ (\pi_2 \circ \pi_3) = (\pi_1 \circ \pi_2) \circ \pi_3$

Gruppen

Wir zeigen, dass $\circ$ auf S_n assoziativ ist.
Es seien $\pi_1, \pi_2, \pi_3 \in S_n$. Wir betrachten die Permutationen
$(\pi_1 \circ \pi_2) \circ \pi_3 = \pi_1 \circ (\pi_2 \circ \pi_3)$.
Um Gleichheit zu zeigen, müssen wir beweisen, dass diese Permutationen die gleiche Zuordnung für jedes $a \in A$ ergeben. Für alle $a \in A$ gilt

$$((\pi_1 \circ \pi_2) \circ \pi_3)(a) = (\pi_1 \circ \pi_2)(\pi_3(a)) = \pi_1(\pi_2(\pi_3(a)))$$

und

$$(\pi_1 \circ (\pi_2 \circ \pi_3))(a) = \pi_1((\pi_2 \circ \pi_3)(a)) = \pi_1(\pi_2(\pi_3(a)))$$

und somit erhalten wir das gleiche Element $\pi_1(\pi_2(\pi_3(a)))$ von A.

Permutationsgruppen

Anwendungen in der Informatik:

- Umordnen von Datenmengen. Durch stellenweises Vertauschen sind alle Reihenfolgen realisierbar.
- **Zusammen mit Ordnungsrelationen: Sortierverfahren**, siehe Vorlesungen zu Algorithmen und Datenstrukturen

Permutationsgruppen

Permutationsgruppen sind also Gruppen. Wir betrachten nun S_3, also die Menge der Permutationen einer Menge mit drei Elementen.
Die **Verknüpfungstafel** lautet:

$\circ$	a	b	c	d	e	f
a	a	b	c	d	e	f
b	b	c	a	e	f	d
c	c	a	b	f	d	e
d	d	f	e	a	c	b
e	e	d	f	b	a	c
f	f	e	d	c	b	a

a ist klarerweise die Identität, und wenn man weiß, dass $b = (1\ 2\ 3)$ und $d = (2\ 3)$ ist, kann man die anderen Elemente berechnen.
Aufgabe: Berechnet die anderen Elemente!
Anmerkungen: $d = (2\ 3)$ bedeutet, dass $1 \to 1$ abgebildet wird; die Tabelle ist so zu lesen: Zeile $i\circ$ Spalte j

Permutationsgruppen

Auflösung:

$a = ()$ (ersichtlich)
$b = (1\ 2\ 3)$ (gegeben)
$c = (1\ 3\ 2)$
$d = (2\ 3)$ (gegeben)
$e = (1\ 2)$
$f = (1\ 3)$

Anmerkungen:

- $(1\ 3\ 2)$ ist dasselbe wie $(3\ 2\ 1)$,
- die Tabelle ist so zu lesen: Zeile $i \circ$ Spalte j

Permutationsgruppen

$c = (1\ 3\ 2)$, denn $b \circ b = c$ und b gegeben
$(1\ 2\ 3) \circ (1\ 2\ 3)$ dh $1 \to 2 \& 2 \to 3$, also $1 \to 3$
$2 \to 3 \& 3 \to 1$, also $2 \to 1$
$3 \to 1 \& 1 \to 2$, also $3 \to 2$

$e = (1\ 2)$, denn $b \circ d = e$ und b und d gegeben
$(1\ 2\ 3) \circ (2\ 3)$ dh $1 \to 1 \& 1 \to 2$, also $1 \to 2$
$2 \to 3 \& 3 \to 1$, also $2 \to 1$
$3 \to 2 \& 2 \to 3$, also $3 \to 3$

$f = (3\ 1)$, denn $b \circ e = f$
$(1\ 2\ 3) \circ (1\ 2)$ dh $1 \to 2 \& 2 \to 3$, also $1 \to 3$
$2 \to 1 \& 1 \to 2$, also $2 \to 2$
$3 \to 3 \& 3 \to 1$, also $3 \to 1$

Restklassen

Wiederholung:

Restklassen: Wir haben schon über Restklassen gesprochen und zwar als wir Äquivalenzklassen betrachtet haben.

Wir erinnern uns:

$R_5 := \{(m, n) \subset \mathbb{Z} \times \mathbb{Z} | m - n \text{ ist ohne Rest durch 5 teilbar } \} \subset \mathbb{Z} \times \mathbb{Z}$

Wir haben dann die 5 Äquivalenzklassen
$[0] := \{0, 5, 10, 15, 20, \dots\}$
$[1] := \{1, 6, \dots\}$
$[2] := \{2, 7, \dots\}$
$[3] := \{3, 8, \dots\}$
$[4] := \{4, 9, \dots\}$
Man schreibt manchmal [5] statt [0] (man könnte auch [735] nehmen)

Restklassen

Man kann die Restklassen auch etwas anders aufschreiben:

$[1] := \{1, 6, \dots\} = 1 + 5 \cdot \mathbb{Z}$

Es hat sich eingebürgert dafür $\mathbb{Z}/n\mathbb{Z}$ zu schreiben und man kann auch Rechenoperationen darauf definieren:

Es gilt:

$$[a] + [b] := [a + b]$$
$$[a] \cdot [b] := [a \cdot b]$$

ZB $[2] + [4] = [2 + 4] = [6] = [1]$
oder $[5] \cdot [3] = [15] = [0] = [5]$

Restklassen

Es gilt: $(\mathbb{Z}/5\mathbb{Z}, +)$ ist eine Gruppe

(G0) $+$ ist eine Verknüpfung auf $\mathbb{Z}/5\mathbb{Z}$

(G1) $[0]$ ist das neutrale Element: $[a] + [0] = [a + 0] = [a]$

(G2) Für $[a]$ ist $[-a]$ das inverse Element: $[a] + [-a] = [a - a] = [0]$

(G3)
$[a]+([b]+[c]) = [a]+[b+c] = [a+b+c] = [a+b]+[c] = ([a]+[b])+[c]$

Restklassen

Anmerkung:
Auch ein Computer rechnet nur in Restklassen, wenn er addiert:
Nehmen wir an eine Zahl wird in einer 16-bit-Integer-Zahl gespeichert.
Eine solche Zahl kann dann maximal eine Größe von $65536 = 2^{16}$ haben.
Wenn wir zu 65536 noch $+1$ rechnen, dann findet ein Überlauf statt und die Zahl ist 0.
$\Rightarrow$ Restklasse $[65537]=[0]$

Ringe

Ringe

Definition:
Ein **Ring** $(R, \oplus, \odot)$ besteht aus einer Menge R mit zwei Verknüpfungen $\oplus$ und $\odot$ auf R mit den folgenden Eigenschaften:

(R1) $(R, \oplus)$ ist eine kommutative Gruppe.

(R2) Für alle $a, b, c \in R$ gilt: $a \odot (b \odot c) = (a \odot b) \odot c$.
(R ist *assoziativ*)

(R3) Für alle $a, b, c \in R$ gilt: $a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$.
Für alle $a, b, c \in R$ gilt: $(b \oplus c) \odot a = (b \odot a) \oplus (c \odot a)$.
(R ist *distributiv*)

Ringe

Definition:
Ein **Ring** $(R, \oplus, \odot)$ heißt außerdem **kommutativ**, wenn zusätzlich gilt:

(R4) Für alle $a, b \in R$ gilt $a \odot b = b \odot a$.

Ringe

Beispiele

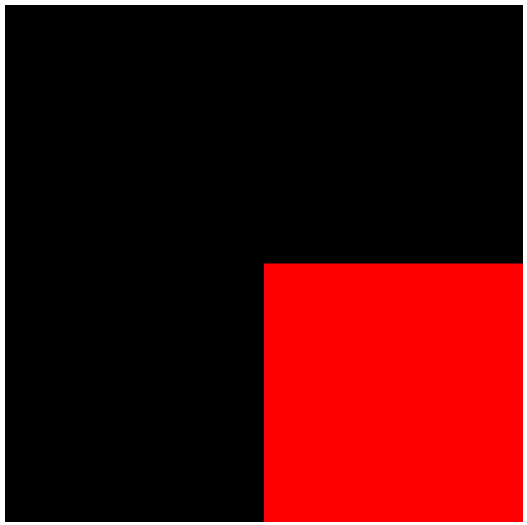
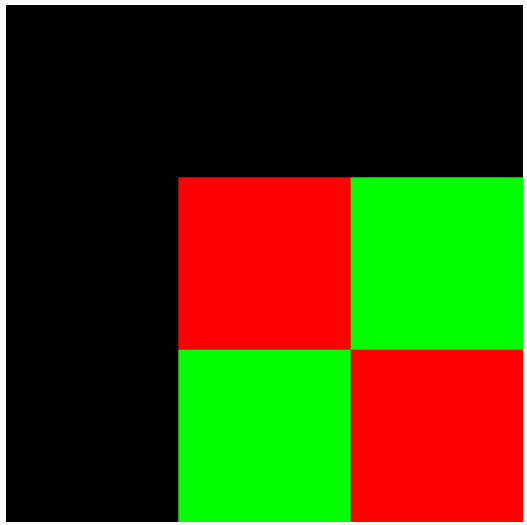
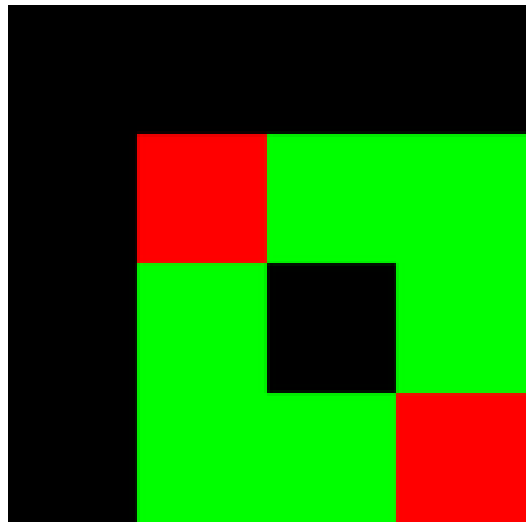
Wir erinnern uns an $\mathbb{Z}/5\mathbb{Z}$ von dem wir gezeigt haben, dass $(\mathbb{Z}/5\mathbb{Z}, +)$ eine Gruppe ist. Man kann zeigen, dass $(\mathbb{Z}/5\mathbb{Z}, +, \cdot)$ sogar ein Ring ist:

(R1) Wir müssen noch zeigen, dass $(\mathbb{Z}/5\mathbb{Z}, +)$ kommutativ ist, also $[a] + [b] = [b] + [a]$.
$[a] + [b] = [a + b] = [b + a] = [b] + [a]$

(R2) $[a] \cdot ([b] \cdot [c]) = [a] \cdot [b \cdot c] = [a \cdot b \cdot c] = [a \cdot b] \cdot [c] = ([a] \cdot [b]) \cdot [c]$.

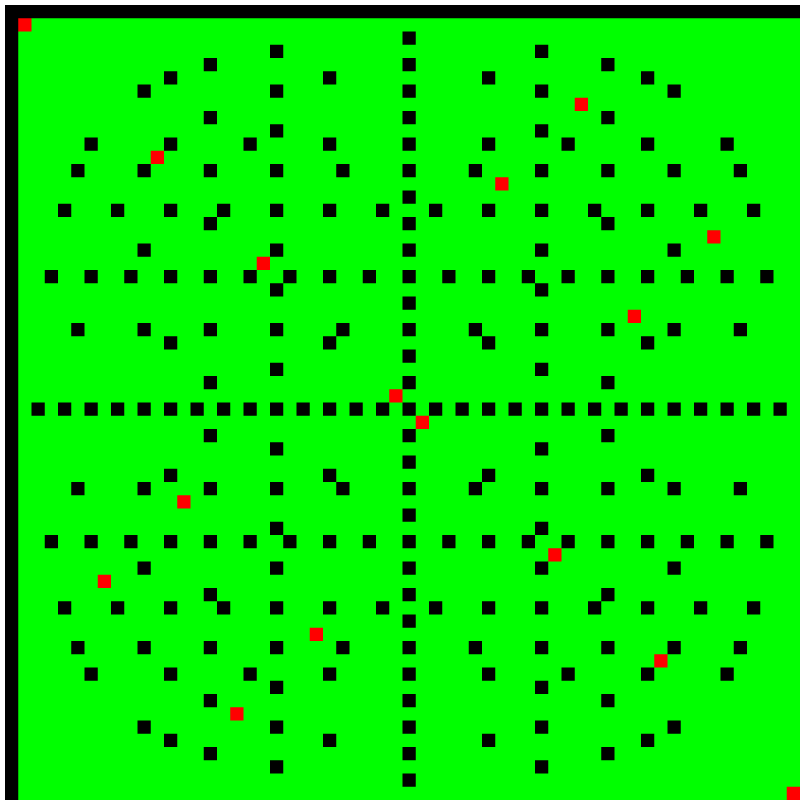
(R3) Zu zeigen ist $[a] \cdot ([b] + [c]) = [a] \cdot [b] + [a] \cdot [c]$ und $([b] + [c]) \cdot [a] = [b] \cdot [a] + [c] \cdot [a]$.

Ringe

Dies ist die Verknüpfungstafel bezüglich der Multiplikation von $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$ und $\mathbb{Z}/4\mathbb{Z}$. Schwarz ist [0] und rot [1]. Grün ist eine Restklasse, die weder [0] noch [1] ist.

Ringe



Das ist die Verknüpfungstafel für $\mathbb{Z}/60\mathbb{Z}$. Auch hier ist schwarz [0] und rot [1]. Grün ist eine Restklasse von [2]-[59].

Körper

Körper

Definition:
Ein **Körper** $(K, \oplus, \odot)$ besteht aus einer Menge K und zwei Verknüpfungen $\oplus$ und $\odot$ auf K mit den folgenden Eigenschaften:

(K1) $(K, \oplus, \odot)$ ist ein kommutativer Ring.

(K2) Es gibt ein Element 1 in K mit $1 \odot a = a \odot 1 = a$ für alle $a \in K$ mit $a \neq 0$.

(K3) Für alle $a \in K$ mit $a \neq 0$ gibt es ein Element $a^{-1} \in K$ mit $a^{-1} \odot a = 1$.

Es gilt also, dass $(K \setminus \{0\}, \odot)$ eine Gruppe ist.

Körper

Definition in kurz:
Ein **Körper** $(K, \oplus, \odot)$ besteht aus einer Menge K und zwei Verknüpfungen $\oplus$ und $\odot$ auf K mit den folgenden Eigenschaften:

1) $(K, \oplus)$ ist eine abelsche Gruppe mit neutralem Element 0.
2) $(K \setminus \{0\}, \odot)$ ist eine abelsche Gruppe mit neutralem Element 1.
3) $a \odot (b \oplus c) = a \odot b \oplus a \odot c$ und $(a \oplus b) \odot c = a \odot c \oplus b \odot c$ für alle $a, b, c \in K$.

Körper

Beispiele:
Körper sind für uns die wichtigsten Strukturen, da die „normale“ Auffassung von Zahlen dem eines Körpers, den reellen Zahlen $\mathbb{R}$, entspricht.

Als Informatiker muss man aber bedenken, dass man eigentlich „nur“ die rationalen Zahlen $\mathbb{Q}$ als Näherung zur Verfügung hat.
Sehr wichtig ist noch der Körper der komplexen Zahlen $\mathbb{C}$, der insbesondere für die Polynomdivision relevant ist, da er **algebraisch abgeschlossen** ist. Mehr dazu später.

Körper

Beispiel:
Ein Körper muss nicht unendlich groß sein: $\mathbb{F}_2$ etwa besteht nur aus den Elementen 0 und 1.

Die Verknüpfungen sind definiert als:

	$+$	$\cdot$
	$0+0=0$	$0 \cdot 0=0$
	$0+1=1$	$0 \cdot 1=0$
	$1+0=1$	$1 \cdot 0=0$
	$1+1=0$	$1 \cdot 1=1$

Ihr kennt $\mathbb{F}_2$ übrigens als $\mathbb{Z}/2\mathbb{Z}$.
Beispiel eines endlichen Körpers (Galoiskörper)

Zusammenfassung

Gruppe $(G, *)$

- Verknüpfung $*$ auf Menge G assoziativ,
- neutrales Element e bzgl. $*$ vorhanden,
- $\forall a \in G$: inverses Element a^{-1} bzgl. $*$ vorhanden.
- optional: $*$ kommutativ (*abelsche Gruppe*)

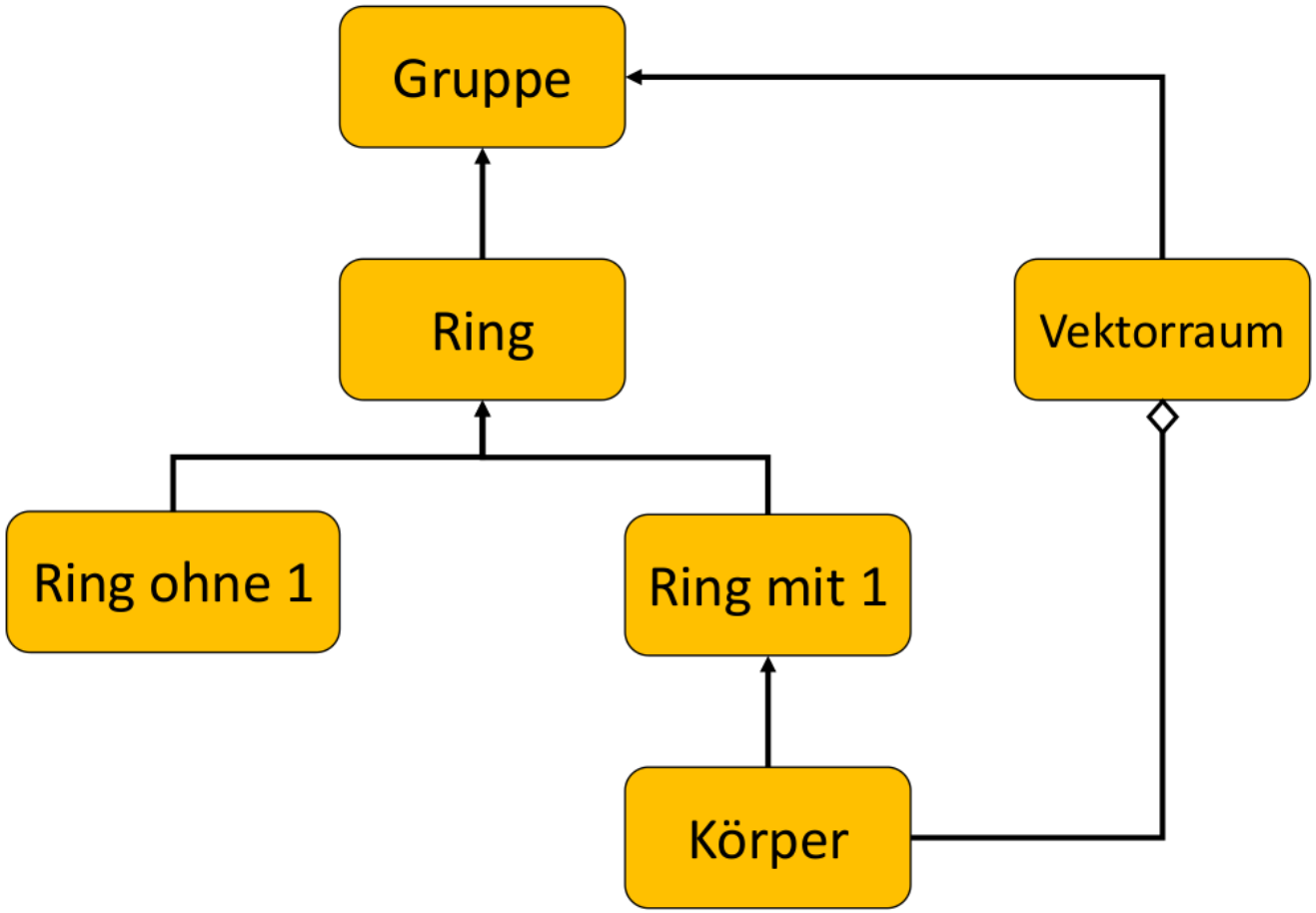
Ring $(R, \oplus, \odot)$

- $(R, \oplus)$ ist abelsche Gruppe,
- Verknüpfung $\odot$ assoziativ,
- Verknüpfungen $\oplus$ und $\odot$ distributiv,
- optional: $\odot$ kommutativ (*kommutativer Ring*), neutrales Element für $\odot$ (*Ring mit 1*)

Körper $(K, \oplus, \odot)$

- $(K, \oplus, \odot)$ ist kommutativer Ring,
- $(K, \oplus)$ ist abelsche Gruppe mit neutralem Element 0,
- $(K \setminus \{0\}, \odot)$ ist abelsche Gruppe mit neutralem Element 1.

Übersicht über algebraische Strukturen



Teilbarkeit und der Algorithmus von Euklid

Teilbarkeit

Definition Teilbarkeit:
Sind $a, b \in \mathbb{Z}$ und ist $b \neq O$ so heißt a durch b teilbar (b teilt a), Notation $b|a$ wenn es eine ganze Zahl q gibt mit $a = b \cdot q$.

Teilbarkeitsregeln:

- Transitivität: $c|b$ und $b|a \Rightarrow c|a$, Beispiel $3|6$ und $6|18 \Rightarrow 3|18$
- $b_1|a_1$ und $b_2|a_2 \Rightarrow b_1 \cdot b_2|a_1 \cdot a_2$, Beispiel: $3|6$ und $4|8 \Rightarrow 12|48$
- $b|a_1$ und $b|a_2 \Rightarrow b|(\lambda \cdot a_1 + \mu \cdot a_2)$,
  Beispiel: $3|6$ und $3|9 \Rightarrow 3|(7 \cdot 6 + 4 \cdot 9)$
- $a|b$ und $b|a \Leftrightarrow a = \epsilon \cdot b$ mit $\epsilon = \pm 1$

Teilbarkeit

Beweis z.B. Transitivität:

$c|b$ und $b|a \Rightarrow b = q_1 \cdot c$ und $a = q_2 \cdot b$

$\Rightarrow a = q_2 \cdot q_1 \cdot c$

$\Rightarrow c|a$

Auch die anderen Eigenschaften lassen sich durch Einsetzen der Definition direkt beweisen.

Teilbarkeit

Beweis der letzten Eigenschaft (andere Richtung analog):
$a|b$ und $b|a \Rightarrow a = \epsilon \cdot b$ mit $\epsilon = \pm 1$ mit $a, b \neq 0$

$a|b$ und $b|a \Rightarrow b = q_1 \cdot a$ und $a = q_2 \cdot b$ *//Definition einsetzen*
$\Rightarrow a = q_2 \cdot q_1 a$*//erste Gleichung in 2. einsetzen*
$\Rightarrow 1 = q_2 \cdot q_1$ *//wegen $a \neq 0$ Kürzen möglich*
$\Rightarrow q_1 = q_2 = \pm 1$ *//wir sind in $\mathbb{Z}$*

Die Zahlen ± 1 heißen Einheiten von $\mathbb{Z}$. Sie sind die einzigen Zahlen die bzgl. der Multiplikation ein Inverses haben.

Größter gemeinsamer Teiler

Definition:
Sind $a, b \in \mathbb{Z}$. Dann heißt $d \in \mathbb{Z}$ **größter gemeinsamer Teiler** (Notation: $ggt(a, b)$ von a und b wenn folgende 2 Bedingungen erfüllt sind:

1. d ist gemeinsamer Teiler von a und b, d.h. $d|a$ und $d|b$
2. für jeden weiteren gemeinsamen Teiler d' von a und b gilt: $d'|d$.

Zwei ganze Zahlen heißen **teilerfremd** wenn $ggt(a, b) = 1$.

Satz:
Für zwei ganze Zahlen a, b gibt es genau eine Zahl d mit $d = ggt(a, b)$.

Beweis der Eindeutigkeit:
Seien d_1 und d_2 zwei größte gemeisame Teiler von a und b. Nach Bedingung 2 gilt dann $d_1|d_2$ und $d_2|d_1$. Daraus folgt $d_1 = \epsilon \cdot d_2$ mit $\epsilon = \pm 1$ wie wir gerade gezeigt haben. Die Existenz zeigen wir gleich.

Teilen mit Rest

Satz: Seien $a, b \in \mathbb{Z},\ b \neq 0$. Dann gibt es eindeutig bestimmte Zahlen $q, r \in \mathbb{Z}$ mit

$$a = q \cdot b + r \text{ und } 0 \leq r < |b|.$$

Beweis der Eindeutigkeit:
Seien $a = q_1 b + r_1$ und $a = q_2 b + r_2$ zwei unterschiedliche Darstellungen. Wir nehmen zusätzlich an: $r_1 \geq r_2$. Jetzt subtrahieren wir die 2. Gleichung von der 1. und erhalten:

$$0 = (q_1 - q_2)b + (r_1 - r_2) \text{ oder } (q_2 - q_1)b = (r_1 - r_2).$$

D.h. $(r_1 - r_2)$ muss durch b teilbar sein. Für die Differenz $(r_1 - r_2)$ von r_i mit $0 \leq r_i < b$ gilt $0 \leq |r_1 - r_2| < b$. Die einzige durch b teilbare natürliche Zahl kleiner als b is also 0. Also ist $r_1 - r_2 = 0$ und dann auch $q_1 - q_2 = 0$. Daher $r_1 = r_2$ und auch $q_1 = q_2$.

Teilen mit Rest

Beweis der Existenz von q und r:
Wegen $qb = (-q)(-b)$ genügt es denn Fall $b > 0$ zu betrachten.
1. Fall: $a > 0$. Wir beweisen durch Induktion über a.

Induktionsanfang $a = 1$: $1 = qb + r$, ist wahr für $b = 1, q = 1, r = 0$.
Induktionsschritt $a \to a + 1$: Nach Induktionsvoraussetzung haben wir eine Darstellung $a = qb + r, 0 \leq r < b$. Daraus folgt:

$$a + 1 = qb + (r + 1).$$

Falls $r + 1 < b$ sind wir fertig. Ansonsten gilt $r + 1 = b$ und wir haben

$$a + 1 = (q + 1)b + 0.$$

Teilen mit Rest

Beweis der Existenz von q und r:
2. Fall: $a < 0$ können wir auf den 1. Fall zurückführen, da $-a > 0$:

$$-a = qb + r \text{ mit } 0 \leq r < b$$

also $a = (-q)b + (-r)$. Falls $r = 0$ sind wir fertig. Ansonsten falls $r > 0$:

$$a = (-q - 1)b + (b - r).$$

Bestimmung des größten gemeinsamen Teilers

Der **Algorithmus von Euklid**

- ist einer der ältesten Algorithmen überhaupt (über 2000 Jahre alt).
- hat alles, was ein Algorithmus braucht: Eingabeparameter, Berechnungsvorschrift, Ergebnis.
- ist ein konstruktiver Beweis für die Existenz des größten gemeinsamen Teilers (die Eindeutigkeit hatten wir bereits gezeigt).

Algorithmus von Euklid

Wir wollen d berechnen mit $d = ggt(a, b)$. Wir setzen $x_0 := a$ und $x_1 := b$ und führen nach dem folgenden Schema sukzessive Teilungen mit Rest durch bis der Rest 0 geworden ist.

$$\begin{array}{rcrcccl} x_0 & = & q_1 x_1 + x_2, & 0 & < & x_2 & < x_1, \\ x_1 & = & q_2 x_2 + x_3, & 0 & < & x_3 & < x_2, \\ & \ldots & & & & & \\ x_{n-2} & = & q_{n-1} x_{n-1} + x_n, & 0 & < & x_n & < x_{n-1}, \\ x_{n-1} & = & q_n x_n + 0. & & & & \end{array}$$

Behauptung: Der letzte Divisor $d := x_n$ ist der gesuchte $ggt(a, b)$. Wir werden das gleich beweisen, schauen uns aber erst an Beispielen an wie der Algorithmus funktioniert.

Algorithmus von Euklid, Beispiel

Berechne $ggt(238, 35)$
Initialisiere die Variablen $x_0 := 238$ und $x_1 = 35$

$$
\begin{array}{rcll}
x_0 & = & q_1 x_1 + x_2, & 0 < x_2 < x_1, \\
238 & = & q_1 \cdot 35 + x_2, & \\
238 & = & 6 \cdot 35 + 28, & \\
x_1 & = & q_2 x_2 + x_3, & 0 < x_3 < x_2, \\
35 & = & q_2 \cdot 28 + x_3 & \\
28 & = & 4 \cdot 7 + 0 &
\end{array}
$$

$ggt(238, 35) = 7$.

Weiteres Beispiel, versuchen Sie es selbst!

Bestimmen Sie $ggt(239, 35)$.

Weiteres Beispiel, versuchen Sie es selbst!

Bestimmen Sie $ggt(239, 35)$.

$$\begin{aligned} 239 &= 6 \cdot 35 + 29 \\ 35 &= 1 \cdot 29 + 6 \\ 29 &= 4 \cdot 6 + 5 \\ 6 &= 1 \cdot 5 + 1 \\ 5 &= 5 \cdot 1 + 0 \end{aligned}$$

$ggt(239, 35) = 1$.

Beobachtung: Die Reste werden umso schneller klein je größer die Quotienten sind. Im schlechtesten Fall sind alle Quotienten 1. Wieviele Schritte braucht der Algorithmus dann?

Der Algorithmus von Euklid und die Fibonacci Zahlen

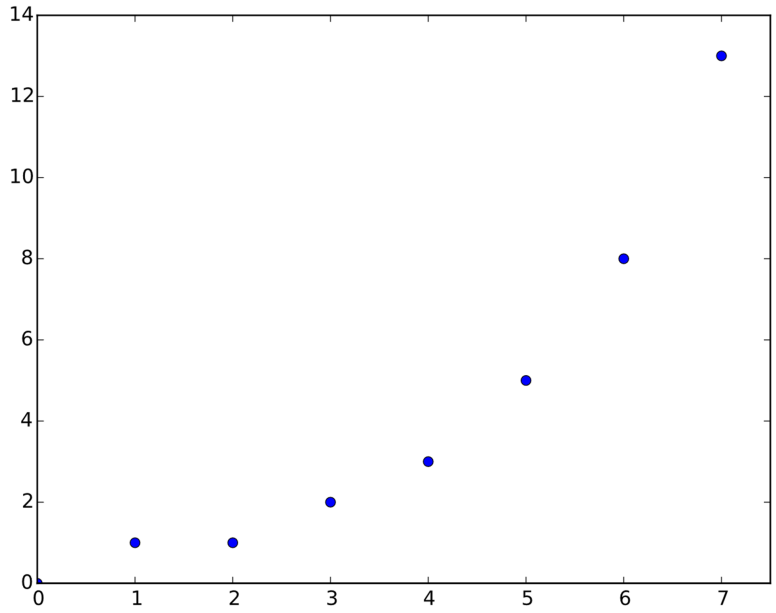
Die **Fibonacci Zahlen** sind eine unendliche Zahlenfolge.
Berechnungsvorschrift:

$$\begin{aligned} f_{n+1} &= 1 \cdot f_n + f_{n-1} \\ f_n &= 1 \cdot f_{n-1} + f_{n-2} \\ &\dots \\ f_3 &= 1 \cdot f_2 + f_1 \\ f_2 &= 1 \cdot f_1 + 0 \end{aligned}$$

Beginn: $f_1 := 1$, daraus folgt: $f_2 = 1$ und so weiter, d.h. $2, 3, 5, 8, 13 \dots$.
Jede Zahl ist Summe der beiden vorhergehenden Zahlen.

Beobachtung: Die Fibonacci Zahlen sind die Folge mit den kleinst möglichen Quotienten, also 1. Zwei aufeinanderfolgende Fibonacci Zahlen sind teilerfremd.

Der Algorithmus von Euklid und die Fibonacci Zahlen



Beobachtung: f_n wächst exponentiell für steigendes n. Daher ist der Algorithmus von Euklid auch im schlechtesten Fall sehr schnell fertig. Genauer: Euklid Agorithmus braucht für $ggt(a, b)$ immer weniger als $O(h)$ Divisionen, wo h ist die Anzahl der Ziffern in der kleineren Zahl b.
Solche Worst-case Laufzeitabschätzungen sind sehr wichtig für die Informatik und basieren oft auf mathematischen Grundlagen!

Das Lemma von Bézout und der erweiterte Euklidsche Algorithmus als konstruktiver Beweis

Satz:
Seien $a, b \in \mathbb{Z}$ und $d = ggt(a, b)$ ihr größter gemeinsamer Teiler. Dann gibt es Zahlen $\lambda, \mu \in \mathbb{Z}$ so dass:

$$d = \lambda \cdot a + \mu \cdot b.$$

Daraus folgt: Zwei ganze Zahlen a und b sind genau dann teilerfremd wenn gilt:

$$d = \lambda \cdot a + \mu \cdot b = 1.$$

Wir beweisen diesen Satz konstruktiv mit einer Erweiterung des Algorithmus von Euklid.

Der erweiterte Euklidsche Algorithmus

Wir setzen wieder $x_0 := a$ und $x_1 := b$ und berechnen genauso wie beim Algorithmus von Euklid:

$$\begin{array}{rcrcccl} x_0 & = & q_1 x_1 + x_2, & 0 & < & x_2 & < x_1, \\ x_1 & = & q_2 x_2 + x_3, & 0 & < & x_3 & < x_2, \\ & \ldots & & & & & \\ x_{n-2} & = & q_{n-1} x_{n-1} + x_n, & 0 & < & x_n & < x_{n-1}, \\ x_{n-1} & = & q_n x_n + 0. & & & & \end{array}$$

Gleichzeitig konstruieren wir Zahlen λ_k, μ_k so dass:
$x_k = \lambda_k a + \mu_k b$ für $k = 0, 1, 2, \ldots n$.
Wir beginnen mit $x_0 = \lambda_0 a + \mu_0 b$. Da $x_0 = a$
ist $(\lambda_0, \mu_0) = (1, 0)$, analog ist $(\lambda_1, \mu_1) = (0, 1)$.

Der erweiterte Euklidsche Algorithmus

Sei (λ_i, μ_i) schon konstruiert für $i \leq k$.
Dann bekommen wir $(\lambda_{k+1}, \mu_{k+1})$ wegen der Gleichung
$x_{k-1} = q_k x_k + x_{k+1}$ durch die Rekursionsformel

$$(\lambda_{k+1}, \mu_{k+1}) = (\lambda_{k-1}, \mu_{k-1}) - q_k(\lambda_k, \mu_k).$$

Da $d = ggt(a, b) = x_n$ erfüllt $(\lambda, \mu) := (\lambda_n, \mu_n)$ die gewünschte Gleichung

$$d = \lambda a + \mu b$$

und das Lemma von Bézout ist bewiesen.

Der erweiterte Euklidsche Algorithmus: Beispiel

Bestimmen Sie $ggt(239, 35)$ und berechnen Sie zusätzlich λ und μ. Setzen Sie zunächst $(\lambda_0, \mu_0) = (1, 0)$ und $(\lambda_1, \mu_1) = (0, 1)$. Dann berechnen Sie jeweils: $(\lambda_{k+1}, \mu_{k+1}) = (\lambda_{k-1}, \mu_{k-1}) - q_k(\lambda_k, \mu_k)$.

$$
\begin{array}{rcl@{\quad}c@{\quad}rcl@{\quad}c@{\quad}rcl}
239 &=& 6 \cdot 35 + 29 & // & (\lambda_2, \mu_2) &=& (1,0) - 6 \cdot (0,1) &=& (1,-6) \\
35 &=& 1 \cdot 29 + 6 & // & (\lambda_3, \mu_3) &=& (0,1) - 1 \cdot (1,-6) &=& (-1,7) \\
29 &=& 4 \cdot 6 + 5 & // & (\lambda_4, \mu_4) &=& (1,-6) - 4 \cdot (1,-7) &=& (5,-34) \\
6 &=& 1 \cdot 5 + 1 & // & (\lambda_5, \mu_5) &=& (-1,7) - 1 \cdot (5,-34) &=& (-6,41) \\
5 &=& 5 \cdot 1 + 0 & & & & & &
\end{array}
$$

Also:

$$1 = ggt(239, 35) = -6 \cdot 239 + 41 \cdot 35$$

Literatur

- Hartmann Kapitel 5.1 (Gruppen), 5.2 (Ringe), 5.3 (Körper), 4.2 (Teilbarkeit)
- Skript zur Vorlesung *Einführung in die Zahlentheorie* von Otto Forster, LMU München 2004