

Kapitel G

Ringe und Körper

Be wise, generalize!
(mathematisches Sprichwort)

The commonly accepted attitudes toward the commutative law and the associative law are different. Many real life operations fail to commute; the mathematical community has learned to live with that fact and even to enjoy it. Violations of the associative law are usually considered by specialists only.

Paul Halmos (1916–2006), *Linear Algebra Problem Book* (1995)

Inhalt dieses Kapitels G

- 1 Monoide und Gruppen
 - Verknüpfungen
 - Monoide und Gruppen
 - Lösung von Gleichungen
 - Untergruppen und -monoide
 - Homomorphismen
 - Erzeugte Untergruppen
 - Kartesische Produkte
- 2 Ringe und Körper
 - Definition und erste Rechenregeln
 - Homomorphismen und Unterringe
 - Matrixringe und Funktionenringe
- 3 Polynomringe
 - Definition und erste Rechenregeln
 - Die universelle Abbildungseigenschaft
 - Euklidische Division und Nullstellen von Polynomen
 - Arithmetik in \mathbb{Z} und $K[X]$ und euklidischen Ringen

Das Ziel in diesem Kapitel sind Ringe und Körper, insbesondere wollen wir Polynomringe behandeln.

Zur Vorbereitung ist es effizient, zunächst die Grundlagen für Monoide und Gruppen zu legen; das ist der erste Teil.

Ich führe dazu die nötigen Vokabeln und ein und erste einfache Rechnungen für Sie aus.

Der Weg ist lang, aus vielen kleinen Schritten, aber er lohnt sich für eine solide Grundlage.

Verknüpfungen: allgemeine Definition

Definition G1A: Verknüpfung / Operation

Gegeben seien Mengen A, B, C . Jede Abbildung

$$* : A \times B \rightarrow C : (a, b) \mapsto c = *(a, b) = (a, b)* = a * b = ab$$

nennen wir **(zweistellige) Verknüpfung** oder **(binäre) Operation**.

Statt **Präfix** $*(a, b)$ oder **Postfix** $(a, b)*$ schreiben wir meist **Infix** $a * b$.

Diese traditionelle **algebraische Schreibweise** ist kurz und bequem.

Statt $a * b$ schreiben wir auch kurz ab , falls die Verknüpfung $*$ aus dem Kontext hervorgeht und keine Missverständnisse zu befürchten sind.

Im Falle $B = C$ heißt $* : A \times B \rightarrow B$ **Linksoperation** von A auf B .

Im Falle $A = C$ heißt $* : A \times B \rightarrow A$ **Rechtsoperation** von B auf A .

Im Falle $A = B$ heißt $* : A \times A \rightarrow C$ eine **(äußere) Verknüpfung** auf A nach C . Sie heißt **kommutativ**, falls $a * b = b * a$ für alle $a, b \in A$ gilt.

Im Falle $A = B = C$ heißt $* : A \times A \rightarrow A$ **(innere) Verknüpfung** auf A . Sie heißt **assoziativ**, falls $(a * b) * c = a * (b * c)$ für alle $a, b, c \in A$ gilt.

Verknüpfungen: allgemeine Definition

Wir sagen **zweistellige Verknüpfung** oder **binäre Operation**, um zu betonen, dass genau zwei Elemente miteinander verknüpft werden.

Assoziativität $(a * b) * c = a * (b * c)$ erlaubt uns, Klammern wegzulassen, und Kommutativität erlaubt uns, Faktoren umzuordnen, siehe Satz G1c.

Eine n -stellige Verknüpfung für $n \in \mathbb{N}$ ist eine Abbildung der Form

$$f : A_1 \times \cdots \times A_n \rightarrow B : (a_1, \dots, a_n) \mapsto b = f(a_1, \dots, a_n).$$

Im Falle $A_1 = \cdots = A_n = B$ nennen wir f eine **innere Verknüpfung**; in allen anderen Fällen ist f einfach eine **(äußere) Verknüpfung**.

Im Falle $n = 0$ ist $f : \{0\} \rightarrow B : 0 \mapsto b$ einfach nur ein **Element** $b \in B$.

Im Falle $n = 1$ ist $f : A_1 \rightarrow B : a \mapsto b = f(a)$ einfach eine **Funktion**.

Im Falle $n = 2$ ist $f : A_1 \times A_2 \rightarrow B$ eine **zweistellige Verknüpfung**.

Im Falle $n = 3$ ist $f : A_1 \times A_2 \times A_3 \rightarrow B$ eine **ternäre Operation**.

Meist betrachten wir Verknüpfungen der Stelligkeit $n \leq 2$, aber auch Verknüpfungen von höherer Stelligkeit kommen vor und sind nützlich. Dies gilt besonders für **Multilinearformen**, die wir später untersuchen.

Verknüpfungen: erste Beispiele

Beispiel: Wir verknüpfen Zähler und Nenner zum Quotienten:

$$/ : \mathbb{Z} \times \mathbb{N}^* \rightarrow \mathbb{Q} : (z, n) \mapsto z/n$$

Beispiel: Die euklidische Division in \mathbb{Z} definiert zwei Verknüpfungen

$$(\text{quo}, \text{rem}) : \mathbb{Z} \times \mathbb{Z}^* \rightarrow \mathbb{Z} \times \mathbb{N} : (a, b) \mapsto (q, r)$$

als eindeutige Lösung der Gleichung $a = bq + r$ mit $0 \leq r < |b|$.

Allgemein zu je zwei reellen Zahlen $a, b \in \mathbb{R}$ mit $b \neq 0$ existiert genau ein Paar (q, r) mit $a = bq + r$ und $q \in \mathbb{Z}$ und $r \in [0, |b|$. Dies definiert

$$(\text{quo}, \text{rem}) : \mathbb{R} \times \mathbb{R}^* \rightarrow \mathbb{Z} \times \mathbb{R}_{\geq 0} : (a, b) \mapsto (q, r).$$

Für $b = 1$ ist somit $a = q + r$ die Zerlegung in den ganzzahligen Teil $q = a \text{ quo } 1 = \lfloor a \rfloor \in \mathbb{Z}$ und den Nachkommanteil $r = a \text{ rem } 1 \in [0, 1$.

Verknüpfungen: erste Beispiele

Beispiele: Für jeden Ring $\mathbb{K} = \mathbb{Z}, \mathbb{Z}_n, \dots$ haben wir die ersten drei, für jeden Körper $\mathbb{K} = \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p, \dots$ alle vier Grundrechenarten

$$\text{Addition} \quad + : \mathbb{K} \times \mathbb{K} \rightarrow \mathbb{K} \quad : (a, b) \mapsto a + b,$$

$$\text{Subtraktion} \quad - : \mathbb{K} \times \mathbb{K} \rightarrow \mathbb{K} \quad : (a, b) \mapsto a - b,$$

$$\text{Multiplikation} \quad \cdot : \mathbb{K} \times \mathbb{K} \rightarrow \mathbb{K} \quad : (a, b) \mapsto a \cdot b,$$

$$\text{Division} \quad / : \mathbb{K} \times \mathbb{K}^* \rightarrow \mathbb{K} \quad : (a, b) \mapsto a/b.$$

Addition und Multiplikation sind hier assoziativ und kommutativ, doch Subtraktion und Division sind i.A. weder assoziativ noch kommutativ:

$$3 - 5 \neq 5 - 3, \quad (8 - 5) - 3 \neq 8 - (5 - 3),$$

$$3/5 \neq 5/3, \quad (8/4)/2 \neq 8/(4/2).$$

Assoziativität und Kommutativität sind keineswegs selbstverständlich! Im Gegenteil sind dies seltene Glücksfälle, die wir wertschätzen sollten. Dank dieser besonderen Eigenschaften können wir effizient rechnen.

Verknüpfungen: erste Beispiele

Beispiel: Ist die Addition von Fließkommazahlen assoziativ?

Hier lohnt sich ein numerisches Experiment, einfach aber eindrücklich:

```

1 a = +1000000000 # +1e+9, eine Milliarde
2 b = -1000000000 # -1e+9, minus eine Milliarde
3 c = 0.000000001 # +1e-9, also ein Milliardstel
4 print( (a + b) + c )
5 print( a + (b + c) )

```

😊 Die Rechnung $(a+b)+c$ ergibt $1e-9$, das ist das korrekte Ergebnis.

☹ Die Rechnung $a+(b+c)$ ergibt 0.0 , das ist ein (Rundungs-)Fehler.

⚠ Fließkommazahlen haben eine feste Zahl von (Nachkomma)Stellen, typischerweise 52 Bits (nach Standard IEEE 754), dazu 11 Bits für den Exponenten und noch eins für das Vorzeichen, also insgesamt 64 Bits. Die Menge dieser Zahlen ist endlich, sie hat höchstens 2^{64} Elemente.

⚠ Selbst mit mehr Bits und potentiell beliebig viel Speicher bleiben die darstellbaren Zahlen abzählbar. Die Menge \mathbb{R} ist jedoch überabzählbar!

Verknüpfungen: erste Beispiele

⚠ Fließkomma-Arithmetik ist deutlich anders als exakte Arithmetik in \mathbb{Q} . Das muss man wissen, um böse Überraschungen zu vermeiden!

Aufgabe: Was liefert folgende Schleife? Wagen Sie eine Vorhersage!

```
1 x = 0.0
2 while x < 1.0: print(x); x += 0.1
```

Wie viele und welche Werte werden angezeigt? Wie erklären Sie das?

⚠ Insbesondere Analysis und Numerik nutzen die reellen Zahlen \mathbb{R} als Grundlage. Alle Rechnungen (Operationen, Funktionen, etc.) sind exakt definiert, aber für praktische Belange meist zu aufwändig. Sie werden daher geeignet approximiert durch kostengünstigere Näherungen.

⚠ Die Numerik auf dem Computer ist nochmal komplizierter als in \mathbb{R} , denn nun sind selbst die grundlegenden Rechnungen (Operationen, Funktionen, etc.) nicht exakt, sondern nur genähert. Die Vermeidung bzw. Beschränkung von Rundungsfehlern ist daher eine eigene Kunst.

Verknüpfungen: erste Beispiele

Beispiele: Für Matrizen über $\mathbb{K} = \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}, \mathbb{Z}_n, \mathbb{H}, \dots$ haben wir

$$+ : \mathbb{K}^{m \times n} \times \mathbb{K}^{m \times n} \rightarrow \mathbb{K}^{m \times n} : (A, B) \mapsto C = A + B, \quad c_{ij} = a_{ij} + b_{ij},$$

$$- : \mathbb{K}^{m \times n} \times \mathbb{K}^{m \times n} \rightarrow \mathbb{K}^{m \times n} : (A, B) \mapsto D = A - B, \quad d_{ij} = a_{ij} - b_{ij}.$$

Diese Addition ist assoziativ und kommutativ, die Subtraktion i.A. nicht. Zwei Matrizen passender Größe können wir multiplizieren vermöge

$$\cdot : \mathbb{K}^{p \times q} \times \mathbb{K}^{q \times r} \rightarrow \mathbb{K}^{p \times r} : (A, B) \mapsto C = A \cdot B, \quad c_{ik} = \sum_{j=1}^q a_{ij} \cdot b_{jk}.$$

Für $p = q = r$ ist die Multiplikation assoziativ, aber i.A. nicht kommutativ. Zudem operiert \mathbb{K} auf $\mathbb{K}^{m \times n}$ von links und von rechts durch Skalierung:

$$\cdot : \mathbb{K} \times \mathbb{K}^{m \times n} \rightarrow \mathbb{K}^{m \times n} : (\lambda, A) \mapsto B = \lambda \cdot A, \quad b_{ij} = \lambda \cdot a_{ij}$$

$$\cdot : \mathbb{K}^{m \times n} \times \mathbb{K} \rightarrow \mathbb{K}^{m \times n} : (A, \lambda) \mapsto C = A \cdot \lambda, \quad c_{ij} = a_{ij} \cdot \lambda$$

Wir betrachten $\mathbb{K}^n \cong \mathbb{K}^{n \times 1} : (a_i) \rightleftarrows (a_{i1})$ meist als Spaltenvektoren, je nach Bedarf $\mathbb{K}^n \cong \mathbb{K}^{1 \times n} : (a_i) \rightleftarrows (a_{1i})$ auch als Zeilenvektoren.

Beispiel: $(\mathbb{K}^n, +, \cdot)$, Addition von Vektoren, Multiplikation mit Skalaren.

Verknüpfungen: erste Beispiele

Beispiele: Die quadratischen Matrizen bilden den Ring

$$(\mathbb{K}^{n \times n}, +, 0_{n \times n}, \cdot, 1_{n \times n}).$$

Dieser operiert von links auf den Spaltenvektoren:

$$\cdot : \mathbb{K}^{n \times n} \times \mathbb{K}^n \rightarrow \mathbb{K}^n : (A, x) \mapsto Ax$$

So formulieren wir lineare Gleichungssysteme bequem als $Ax = y$.

Die invertierbaren Matrizen bilden die allgemeine lineare Gruppe

$$\begin{aligned} \text{GL}_n(\mathbb{K}) &:= (\mathbb{K}^{n \times n}, \cdot, 1_{n \times n})^\times \\ &= \{ A \in \mathbb{K}^{n \times n} \mid \exists B \in \mathbb{K}^{n \times n} : A \cdot B = B \cdot A = 1_{n \times n} \}. \end{aligned}$$

Diese Gruppe operiert auf Matrizen von links und von rechts:

$$\begin{aligned} \cdot : \text{GL}_m \mathbb{K} \times \mathbb{K}^{m \times n} &\rightarrow \mathbb{K}^{m \times n} : (S, A) \mapsto S \cdot A \\ \cdot : \mathbb{K}^{m \times n} \times \text{GL}_n \mathbb{K} &\rightarrow \mathbb{K}^{m \times n} : (A, T) \mapsto A \cdot T \end{aligned}$$

Das entspricht den Zeilen/Spaltenoperationen im Gauß-Algorithmus.

Verknüpfungen: erste Beispiele

Jede Verknüpfung $*$: $A \times B \rightarrow C$: $(a, b) \mapsto a * b$ entspricht einer Tabelle: Jedem Paar $(a, b) \in A \times B$ wird sein Produkt $a * b$ in C zugeordnet.

😊 Kleine Verknüpfungstabellen können wir explizit ausschreiben.

Beispiele: So definieren wir die logischen Verknüpfungen:

\wedge	0	1
0	0	0
1	0	1

\vee	0	1
0	0	1
1	1	1

$\dot{\vee}$	0	1
0	0	1
1	1	0

\Rightarrow	0	1
0	1	1
1	0	1

\Leftrightarrow	0	1
0	1	0
1	0	1

Beispiel: Allgemein ist ein Junktor eine n -stellige Verknüpfung

$$J : \{0, 1\}^n \rightarrow \{0, 1\} : a \mapsto J(a).$$

Dies können wir als Wahrheitstabelle darstellen. Beliebige große Tabellen sind im Prinzip möglich, aber mit wachsenden Kosten. (P = NP? C1κ)

Jede n -stellige Verknüpfung $J : \{0, 1\}^n \rightarrow \{0, 1\}$ können als eine Formel in den Verknüpfungen \wedge, \vee, \neg darstellen (CNF / DNF, siehe Satz C1H).

Verknüpfungen: erste Beispiele

Beispiele: Verknüpfungstabellen für $\mathbb{Z}_n \cong \mathbb{Z}/n\mathbb{Z}$:

$+_2$	0	1
0	0	1
1	1	0

Körper!

$+_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Körper!

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

CRing!

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Körper!

\cdot_2	0	1
0	0	0
1	0	1

\cdot_3	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

\cdot_4	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

\cdot_5	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Verknüpfungen: erste Beispiele

Beispiele: Wir kennen und nutzen ebenso Operationen auf Mengen:

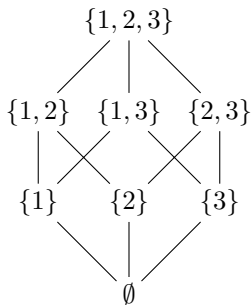
Vereinigung $\cup : \mathfrak{P}(X) \times \mathfrak{P}(X) \rightarrow \mathfrak{P}(X) : (A, B) \mapsto A \cup B$

Durchschnitt $\cap : \mathfrak{P}(X) \times \mathfrak{P}(X) \rightarrow \mathfrak{P}(X) : (A, B) \mapsto A \cap B$

sym. Differenz $\Delta : \mathfrak{P}(X) \times \mathfrak{P}(X) \rightarrow \mathfrak{P}(X) : (A, B) \mapsto A \Delta B$

Differenz $\setminus : \mathfrak{P}(X) \times \mathfrak{P}(X) \rightarrow \mathfrak{P}(X) : (A, B) \mapsto A \setminus B$

Die ersten drei sind kommutativ und assoziativ, die vierte jedoch nicht.
Im Hasse-Diagramm gilt $A \cap B = \inf\{A, B\}$ und $A \cup B = \sup\{A, B\}$:



Verknüpfungen: erste Beispiele

Es gibt zahllose weitere Beispiele von Verknüpfungen, sowohl innere als auch äußere. In die große Vielfalt wollen wir etwas Ordnung bringen, wichtige Eigenschaften benennen und grundlegend untersuchen. Wir wollen Werkzeuge bereitstellen, um damit effizient zu arbeiten.

Definition G1B: Vertauschung und Kommutativität

Zu $*$: $A \times B \rightarrow C$ definieren wir die **entgegengesetzte Verknüpfung**

$$\bar{*} = *^{\text{op}} : B \times A \rightarrow C : (b, a) \mapsto b \bar{*} a = a * b.$$

Beide fassen wir übersichtlich als Diagramm zusammen:

$$\begin{array}{ccccc}
 (a, b) \in & A & \times & B & \xrightarrow[\quad (a,b) \mapsto a*b \quad]{*} & C \\
 \tau_{A,B} \updownarrow & \searrow \text{id} & & \swarrow \text{id} & & \downarrow \text{id} \\
 & & & & & \\
 (b, a) \in & B & \times & A & \xrightarrow[\quad (b,a) \mapsto b\bar{*}a \quad]{\bar{*}} & C
 \end{array}$$

Die Verknüpfung $*$ heißt **kommutativ** oder **symmetrisch**, falls $\bar{*} = *$. Ausführlich bedeutet das: Es gilt $A = B$ und $a * b = b * a$ für alle $a, b \in A$. Anschaulich gesagt: Es gilt $A = B$, und die Verknüpfungstabelle von $*$: $A \times A \rightarrow C$ ist spiegelsymmetrisch bezüglich der Hauptdiagonalen.

Vertauschung und Kommutativität

Zu jeder Verknüpfung $* : A \times B \rightarrow C$ haben wir die entgegengesetzte Verknüpfung $\bar{*} : B \times A \rightarrow C$ (G1B), diese ist definiert durch $b \bar{*} a = a * b$ für alle $b \in B$ und $a \in A$. Die beiden Argumente werden also vertauscht; dies definiert zu $*$ eine neue Verknüpfung $\bar{*}$ mit demselben Ergebnis.

Die Vertauschung von (a, b) zu (b, a) entspricht dem Bijektionspaar

$$\begin{aligned}\tau_{A,B} &: A \times B \xrightarrow{\sim} B \times A : (a, b) \mapsto (b, a), \\ \tau_{B,A} &: B \times A \xrightarrow{\sim} A \times B : (b, a) \mapsto (a, b).\end{aligned}$$

Somit gilt $\bar{*} = * \circ \tau_{B,A}$ und umgekehrt $* = \bar{*} \circ \tau_{A,B}$, wie im obigen Diagramm dargestellt. Insbesondere gilt $\bar{\bar{*}} = *$, also $(*^{\text{op}})^{\text{op}} = *$.

Anschaulich stellen wir uns die kartesischen Produktmengen $A \times B$ und $B \times A$ als Rechtecke vor. Die Vertauschung $(\tau_{A,B}, \tau_{B,A}) : A \times B \cong B \times A$ entspricht der Spiegelung an der Hauptdiagonalen. Der Übergang von $*$ zu $\bar{*}$ entspricht demnach der Spiegelung der Verknüpfungstabelle.

Beispiel: Komposition von Abbildungen

Beispiel: Zu je drei Mengen X, Y, Z haben wir die Komposition

- : $\text{Abb}(X, Y) \times \text{Abb}(Y, Z) \rightarrow \text{Abb}(X, Z) : (f, g) \mapsto f \bullet g,$
- : $\text{Abb}(Y, Z) \times \text{Abb}(X, Y) \rightarrow \text{Abb}(X, Z) : (g, f) \mapsto g \circ f.$

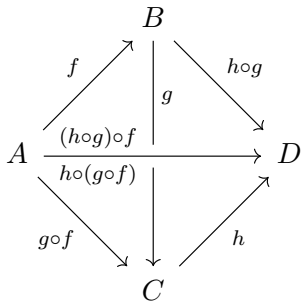
Diese beiden Verknüpfungen sind entgegengesetzt: $f \bullet g = g \circ f$.
Je nach Kontext sind beide Schreibweisen bequem und nützlich.

Erinnerung (D2A): Zu je zwei Abbildungen $f: X \rightarrow Y$ und $g: Y \rightarrow Z$ ist die **Komposition** $h = f \bullet g = g \circ f$ die Abbildung $h: X \rightarrow Z$ durch Hintereinanderausführung $h(x) = g(f(x))$, also $f \bullet g$ als „ f vor g “ und $g \circ f$ als „ g nach f “. Demnach gilt $\bar{\circ} = \bullet$ und entsprechend $\bar{\bullet} = \circ$.

Beispiel: Komposition von Abbildungen

Die Komposition von Abbildungen ist assoziativ:

Für je drei komponierbare Abbildungen $f: A \rightarrow B$ und $g: B \rightarrow C$ und $h: C \rightarrow D$ gilt die Gleichheit der Kompositionen $h \circ (g \circ f) = (h \circ g) \circ f$.



Verknüpfungen: Umklammern und Umordnen

Zu $* : A \times A \rightarrow A$ definieren wir die n -fache Verknüpfung für $n \in \mathbb{N}_{\geq 1}$:

$$* : A^1 \rightarrow A : (a_1) \quad \mapsto a_1$$

$$* : A^2 \rightarrow A : (a_1, a_2) \quad \mapsto a_1 * a_2$$

$$* : A^3 \rightarrow A : (a_1, a_2, a_3) \quad \mapsto (a_1 * a_2) * a_3$$

$$* : A^4 \rightarrow A : (a_1, a_2, a_3, a_4) \quad \mapsto ((a_1 * a_2) * a_3) * a_4$$

...

$$* : A^n \rightarrow A : (a_1, a_2, \dots, a_n) \mapsto \ast_{i=1}^n a_i = (\dots ((a_1 * a_2) * a_3) \dots) * a_n$$


Diese Abbildungen definieren wir rekursiv für alle $n \in \mathbb{N}_{\geq 1}$ durch


$$\ast_{i=1}^1 a_i := a_1, \quad \ast_{i=1}^{n+1} a_i := (\ast_{i=1}^n a_i) * a_{n+1}$$

Satz G1c: Umklammern und Umordnen

- (1) Ist $* : A \times A \rightarrow A$ assoziativ, so ist das Produkt $a_1 * a_2 * \dots * a_n$ klammer-unabhängig: Jede Klammerung führt zum selben Ergebnis.
- (2) Ist $*$ zudem kommutativ, so können wir Faktoren beliebig umordnen.

Verknüpfungen: Umklammern und Umordnen

 Im Allgemeinen sind dabei Reihenfolge und Klammerung wichtig! Hier sind Assoziativität und Kommutativität höchst willkommene Hilfen: Diesen unscheinbaren Satz verwenden wir nahezu in jeder Rechnung!

 Kommutativität allein genügt noch nicht zur Umordnung. Wir benötigen zunächst Assoziativität als Voraussetzung, um die Klammern beliebig setzen zu können.

Beispiel: (siehe C405) Wir suchen eine geschlossene Formel für

$$S(n) := \sum_{k=1}^n k = 1 + 2 + \cdots + n.$$

Dank Assoziativität und Kommutativität erhalten wir

$$\begin{aligned} 2S(n) &= (1 + 2 + \cdots + n-1 + n) + (1 + 2 + \cdots + n-1 + n) \\ &= (1 + 2 + \cdots + n-1 + n) + (n + n-1 + \cdots + 2 + 1) \\ &= (1 + n) + (2 + n-1) + \cdots + (n-1 + 2) + (n + 1) \\ &= n(n + 1) \end{aligned}$$

Daraus folgt die ersehnte geschlossene Formel $S(n) = n(n + 1)/2$.

Verknüpfungen: Umklammern und Umordnen

Beweis: (1) Ist $*$ assoziativ, so ist das Produkt $a_1 * a_2 * \cdots * a_n$ klammer-unabhängig: Jede Klammerung führt zum selben Ergebnis.

Wir präzisieren dies wie folgt: Für alle $2 \leq k \leq n$ in \mathbb{N} gilt

$$\ast_{i=1}^n a_i = (\ast_{i=1}^{k-1} a_i) * (\ast_{i=k}^n a_i).$$

Für $n = 3$ verdanken wir dies der Definition bzw. der Assoziativität:

$$\ast_{i=1}^3 a_i \stackrel{\text{Def}}{=} (a_1 * a_2) * a_3 \stackrel{\text{Ass}}{=} a_1 * (a_2 * a_3)$$

Allgemein für $n \geq 3$ beweisen wir die Aussage per Induktion über n . Für $k = n$ ist dies die Definition, und für alle k mit $2 \leq k < n$ gilt:

$$\begin{aligned} \ast_{i=1}^n a_i &\stackrel{\text{Def}}{=} (\ast_{i=1}^{n-1} a_i) * a_n \stackrel{\text{Ind}}{=} [(\ast_{i=1}^{k-1} a_i) * (\ast_{i=k}^{n-1} a_i)] * a_n \\ &\stackrel{\text{Ass}}{=} (\ast_{i=1}^{k-1} a_i) * [(\ast_{i=k}^{n-1} a_i) * a_n] \stackrel{\text{Def}}{=} (\ast_{i=1}^{k-1} a_i) * (\ast_{i=k}^n a_i) \end{aligned}$$

😊 Per Induktion über n schließen wir: Für jedes Produkt der Länge n in $(A, *)$ ist das Ergebnis unabhängig von der Klammerung.

Verknüpfungen: Umklammern und Umordnen

(2) Ist $*$: $A \times A \rightarrow A$ assoziativ und kommutativ, so können wir Produkte beliebig umordnen: Für jede Umordnung $\{i_1, \dots, i_n\} = \{1, \dots, n\}$ gilt

$$a_{i_1} * a_{i_2} * \dots * a_{i_n} = a_1 * a_2 * \dots * a_n.$$

Für $n = 2$ ist dies die Definition der Kommutativität. Allgemein für $n \geq 2$ führen wir Induktion über n . Es gibt genau ein k mit $i_k = n$, also gilt:

$$\begin{aligned} a_{i_1} * a_{i_2} * \dots * a_{i_n} &\stackrel{(1)}{=} (a_{i_1} * \dots * a_{i_{k-1}}) * (a_{i_k} * a_{i_{k+1}} * \dots * a_{i_n}) \\ &\stackrel{(1)}{=} (a_{i_1} * \dots * a_{i_{k-1}}) * [a_{i_k} * (a_{i_{k+1}} * \dots * a_{i_n})] \\ &\stackrel{\text{Com}}{=} (a_{i_1} * \dots * a_{i_{k-1}}) * [(a_{i_{k+1}} * \dots * a_{i_n}) * a_n] \\ &\stackrel{\text{Ass}}{=} [(a_{i_1} * \dots * a_{i_{k-1}}) * (a_{i_{k+1}} * \dots * a_{i_n})] * a_n \\ &\stackrel{(1)}{=} (a_{i_1} * \dots * a_{i_{k-1}} * a_{i_{k+1}} * \dots * a_{i_n}) * a_n \\ &\stackrel{\text{Ind}}{=} (a_1 * \dots * a_{n-1}) * a_n \\ &\stackrel{\text{Def}}{=} a_1 * a_2 * \dots * a_n \end{aligned}$$



Damit ist auch die Invarianz unter Umordnung bewiesen.

QED

Komplexoperation: elementweise Verknüpfung von Mengen

Zur Verknüpfung von Mengen nutzen wir die bequeme Schreibweise

$$2\mathbb{N} = 2 \cdot \mathbb{N} = \{2 \cdot n \mid n \in \mathbb{N}\} = \{0, 2, 4, 6, 8, \dots\},$$

$$2\mathbb{N} + 1 = 2 \cdot \mathbb{N} + 1 = \{2 \cdot n + 1 \mid n \in \mathbb{N}\} = \{1, 3, 5, 7, 9, \dots\}.$$

Hier werden Mengen elementweise verknüpft. Ausführlich bedeutet das:

Definition G1D: Komplexoperation

Jede Verknüpfung setzen wir fort von Elementen auf Teilmengen:

$$* : A \times B \rightarrow C : (a, b) \mapsto a * b$$

$$* : A \times \mathfrak{P}(B) \rightarrow \mathfrak{P}(C) : (a, T) \mapsto a * T := \{a * b \mid b \in T\}$$

$$* : \mathfrak{P}(A) \times B \rightarrow \mathfrak{P}(C) : (S, b) \mapsto S * b := \{a * b \mid a \in S\}$$

$$* : \mathfrak{P}(A) \times \mathfrak{P}(B) \rightarrow \mathfrak{P}(C) : (S, T) \mapsto S * T := \{a * b \mid a \in S, b \in T\}$$

$$= \bigcup_{a \in S} a * T = \bigcup_{b \in T} S * b$$

Als Spezialfälle erhalten wir $\{a\} * T = a * T$ und $S * \{b\} = S * b$.

Beispiel: In dieser Schreibweise gilt $\mathbb{N} + \mathbb{N} = \mathbb{N}$ und $\mathbb{N} - \mathbb{N} = \mathbb{Z}$.

Komplexoperation: elementweise Verknüpfung von Mengen

Formal handelt es sich hier um vier verschiedene Verknüpfungen, denn die Definitionsmengen sind offensichtlich verschieden: Verknüpft werden einmal Elemente, andermal Teilmengen! Zur Betonung und besseren Unterscheidung nutzen manche Autoren zwei verschiedene Symbole:

$$* : A \times B \rightarrow C : (a, b) \mapsto a * b$$

$$\circledast : \mathfrak{P}(A) \times \mathfrak{P}(B) \rightarrow \mathfrak{P}(C) : (S, T) \mapsto S \circledast T := \{ a * b \mid a \in S, b \in T \}$$

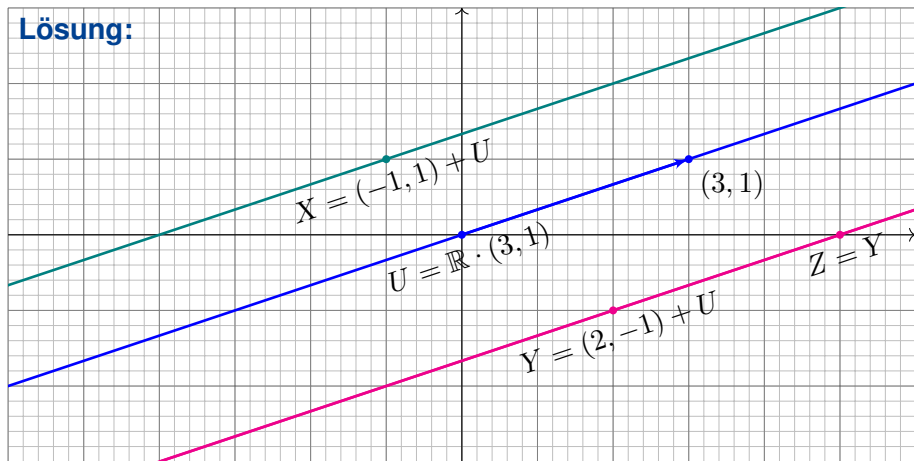
Ich verzichte auf die Betonung und schreibe viermal dasselbe Symbol. aus dem Kontext geht jeweils eindeutig hervor, was genau gemeint ist. Das ist zwar etwas schludrig, aber ein gängiger Kompromiss zwischen Kürze und Klarheit, solange es zu keinen Missverständnissen führt.

Dieses **Überladen** mathematischer Operatoren ist üblich und bequem: Wir hätten gar nicht genug Symbole für all die unzähligen Operationen, schon die Grundrechenarten in $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ müssten verschieden heißen! Programmiersprachen wie Python und C++ nutzen Überladen ebenfalls: Derselbe Operator erfüllt verschiedene Rollen, der Kontext bestimmt die Bedeutung: Diese wird syntaktisch am **Typ der Operanden** erkannt.

Komplexoperation: elementweise Verknüpfung von Mengen

Aufgabe: Zeichnen Sie in der Ebene \mathbb{R}^2 die Mengen $U = \mathbb{R} \cdot (3, 1)$ sowie $X = (-1, 1) + U$ und $Y = (2, -1) + U$ und $Z = (5, 0) + U$.

Lösung:



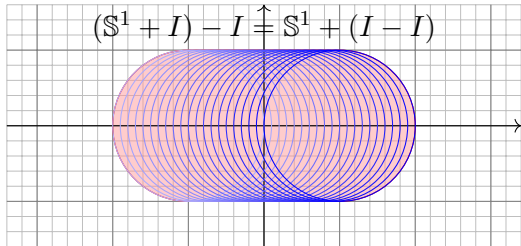
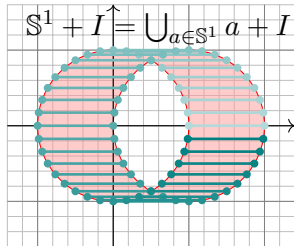
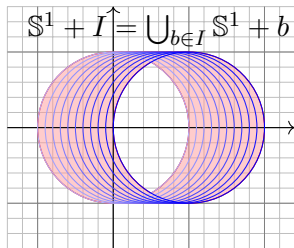
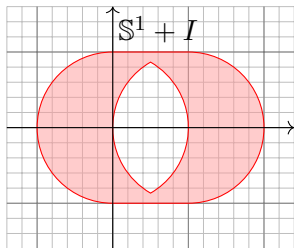
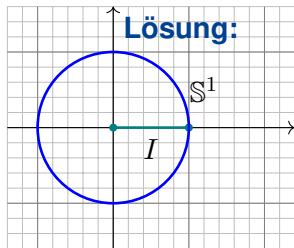
Komplexoperation: elementweise Verknüpfung von Mengen

Hier ist $U = \mathbb{R} \cdot (3, 1) = \{ t \cdot (3, 1) \mid t \in \mathbb{R} \}$ eine Ursprungsgerade und X, Y, X sind Verschiebungen. Man beachte $(2, -1) + U = (5, 0) + U$.

Diese Notation und speziell die Anwendung auf Geraden, Ebenen, usw. ist typisch für die Lineare Algebra. Die folgenden Beispiele zeigen dazu analoge Konstruktionen, die nicht von Geraden handeln, sondern von anderen Mengen wie Intervallen, Kreisen, usw.

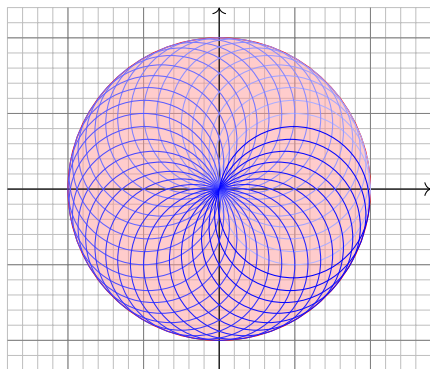
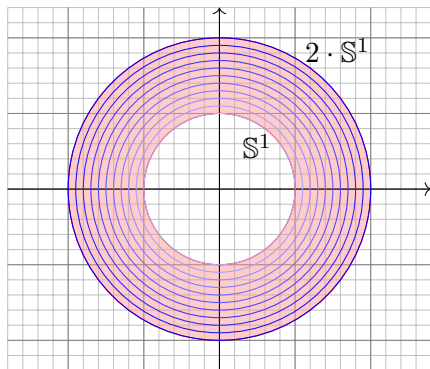
Komplexoperation: elementweise Verknüpfung von Mengen

Aufgabe: Zeichnen Sie in der Ebene \mathbb{R}^2 die Mengen $I = [0, 1] \times \{0\}$ und $S^1 = \{ (x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1 \}$ sowie $S^1 + I$ und $(S^1 + I) - I$.



Komplexoperation: elementweise Verknüpfung von Mengen

Aufgabe: Zeichnen Sie $[1, 2] \cdot \mathbb{S}^1$ und $\mathbb{S}^1 + \mathbb{S}^1$. **Lösung:**



⚠ Beachten Sie $2 \cdot \mathbb{S}^1 \neq \mathbb{S}^1 + \mathbb{S}^1$! Lesen Sie nochmals Definition G1D.

😊 Mathematische Notation ist extrem knapp, präzise und elegant.
In nur wenigen Zeichen können Sie damit viel zusammenfassen.

Bemerkung G1E

- (1) Ist $*$: $A \times A \rightarrow C$ kommutativ, so auch $*$: $\mathfrak{P}(A) \times \mathfrak{P}(A) \rightarrow \mathfrak{P}(C)$.
 (2) Ist $*$: $A \times A \rightarrow A$ assoziativ, so auch $*$: $\mathfrak{P}(A) \times \mathfrak{P}(A) \rightarrow \mathfrak{P}(A)$.

Aufgabe: Schreiben Sie diese Rechnungen sorgfältig aus

Lösung: (1) Wir schreiben die Definition aus und vergleichen:

$$S * T = \{ a * b \mid a \in S, b \in T \}$$

$$T * S = \{ b * a \mid b \in T, a \in S \}$$

Ist $*$: $A \times A \rightarrow C$ kommutativ, so sind die rechten Mengen gleich.

(2) Wir schreiben die Definition aus und vergleichen:

$$(S * T) * U = \{ a * b \mid a \in S, b \in T \} * U$$

$$= \{ (a * b) * c \mid a \in S, b \in T, c \in U \}$$

$$S * (T * U) = S * \{ b * c \mid b \in T, c \in U \}$$

$$= \{ a * (b * c) \mid a \in S, b \in T, c \in U \}$$

Ist $*$: $A \times A \rightarrow A$ assoziativ, so sind die rechten Mengen gleich.

Komplexoperation: elementweise Verknüpfung von Mengen

Anwendungen der Komplexoperation:

- Rechnen mit Restklassen in $\mathbb{Z}/n\mathbb{Z}$, allgemein Quotienten.
- Minkowski-Summe $A + B$ im \mathbb{R}^n wie in obigen Beispielen.
- Fehlerrechnung und Intervallarithmetik

Beispiel: Sie wollen das Volumen eines Quaders schätzen. Sie kennen die Seitenlängen a, b, c nicht exakt, sondern können nur Intervalle angeben, etwa $A = [4.2, 4.4]$, $B = [5.9, 6.2]$, $C = [6.1, 6.2]$. Dann liegt das gesuchte Volumen im Intervall $A \cdot B \cdot C = [151.158, 169.136]$.

😊 Algebra rechnet exakt. „Aber in der Wirklichkeit ist nichts exakt. Das kann die Algebra nicht abbilden.“ Ja, in der Wirklichkeit ist kaum etwas exakt. Doch, wir können Ungenauigkeit algebraisch fassen!

Beispiel: In der Physik werden Messfehler bzw. Vertrauensintervalle in der Schreibweise $m \pm \Delta m$ angegeben. Das entspricht dem Intervall $[m - \Delta m, m + \Delta m]$. Die Verknüpfungen von fehlerbehafteten Werten geschieht dann wie oben gesehen.

Monoide und Gruppen: explizite Definition

Definition G1F: Monoid und Gruppe, explizite Formulierung

Ein **Magma** $(G, *)$ besteht aus einer Menge G mit innerer Verknüpfung

$$* : G \times G \rightarrow G : (a, b) \mapsto a * b.$$

Die Anzahl $\#G = |G|$ der Elemente heißt auch die **Ordnung** von G .

(G0) Eine **Halbgruppe** $(G, *)$ erfüllt zudem die Assoziativität:

$$\mathbf{Ass}(G, *) \quad :\Leftrightarrow \quad \forall a, b, c \in G : (a * b) * c = a * (b * c)$$

(G1) Ein **Monoid** $(G, *, e)$ besitzt zudem ein neutrales Element $e \in G$:

$$\mathbf{Ntr}(G, *, e) \quad :\Leftrightarrow \quad \forall a \in G : e * a = a = a * e$$

$$\mathbf{Mon}(G, *, e) \quad :\Leftrightarrow \quad \mathbf{Ass}(G, *) \wedge \mathbf{Ntr}(G, *, e)$$

(G2) Eine **Gruppe** $(G, *, e, \iota)$ besitzt zudem eine Inversion $\iota : G \rightarrow G$:

$$\mathbf{Inv}(G, *, e, \iota) \quad :\Leftrightarrow \quad \forall a \in G : a * \iota(a) = e = \iota(a) * a$$

$$\mathbf{Grp}(G, *, e, \iota) \quad :\Leftrightarrow \quad \mathbf{Ass}(G, *) \wedge \mathbf{Ntr}(G, *, e) \wedge \mathbf{Inv}(G, *, e, \iota)$$

(GA) Wir nennen $(G, *)$ **kommutativ** oder **abelsch**, falls gilt:

$$\mathbf{Com}(G, *) \quad :\Leftrightarrow \quad \forall a, b \in G : a * b = b * a$$

Monoide und Gruppen: explizite Definition

Wir betrachten hier eine grundlegende **algebraische Struktur** $(G, *)$ bestehend aus einer Menge G und einer Verknüpfung $* : G \times G \rightarrow G$.

Eigenschaften wie Assoziativität **Ass** und Kommutativität **Com** usw. sind **Aussageformen**: Für eine vorgelegte Struktur $(G, *)$ können die Aussagen **Ass** $(G, *)$ und **Com** $(G, *)$ wahr oder falsch sein.

😊 Die obige Definition verlangt explizit alle vier Gruppendaten:

$$\mathbf{Grp}(G, *, e, \iota) \iff \mathbf{Ass}(G, *) \wedge \mathbf{Ntr}(G, *, e) \wedge \mathbf{Inv}(G, *, e, \iota)$$

Die geforderten Eigenschaften sind dann Allaussagen. Das ist gut zu prüfen, alle Daten liegen vor, wir müssen nichts erfinden oder suchen.

Wir wandeln die explizite Definition G1F in eine implizite Definition G1I.

M Beide Sichtweisen sind bequem und nützlich, je nach Situation.

I Für die Programmierung benötigen wir explizite Funktionen.

L *Beautiful is better than ugly. Explicit is better than implicit.*

Monoide und Gruppen: Schreibweisen

Die meisten der algebraischen Strukturen, die uns in der Linearen Algebra begegnen, sind assoziativ, viele davon zudem kommutativ. Nicht-assoziative kommen ebenfalls vor, ein besonders wichtiges Beispiel sind Lie–Algebren, doch insgesamt sind dies eher seltene Ausnahmen. Diese Einschätzung gründet teilweise auf mathematischer Notwendigkeit, vor allem aber auf Tradition und langer Erfahrung.

The commonly accepted attitudes toward the commutative law and the associative law are different. Many real life operations fail to commute; the mathematical community has learned to live with that fact and even to enjoy it. Violations of the associative law are usually considered by specialists only.

Paul Halmos, *Linear Algebra Problem Book* (1995)

Monoide und Gruppen: Schreibweisen

Neben der obigen Schreibweise $(G, *, e, \iota)$ sind weitere üblich:
Additive Schreibweise $(G, +, 0, -)$ mit „Plus“, „Null“, „Negation“.
Multiplikative Schreibweise $(G, \cdot, 1, ^{-1})$ mit „Mal“, „Eins“, „Inversion“.
Ebenso Verknüpfungen $*, \circ, \bullet, \dots$, neutrale Elemente $e, \text{id}, E, I, \dots$

Eine gute Notation vermeidet Fehler und Missverständnisse. Das ist nicht nur eine mathematische Frage, sondern vor allem eine der Klarheit, der Bequemlichkeit und der jeweiligen Tradition. Die wahre Kraft der Begriffe steckt nicht in ihrer *Schreibung*, sondern in ihrer *Bedeutung*! Das können wir nun klar und präzise formulieren.

Beispiele mit 0, 1 und 2 Elementen

Ein Magma $(M, *)$ oder eine Halbgruppe kann leer sein:

Auf $M = \emptyset$ gilt es genau eine Verknüpfung $*: \emptyset \times \emptyset \rightarrow \emptyset$.

Dieses Beispiel ist zwar traurig, aber nicht ausgeschlossen.

Ein Monoid $(M, *, e)$ oder eine Gruppe hingegen ist niemals leer.

Wegen $e \in M$ enthält die Menge M mindestens ein Element.

Auf $M = \{e\}$ gilt es genau eine Verknüpfung $*: \{e\} \times \{e\} \rightarrow \{e\}$.

Damit ist $(M, *, e)$ ein Monoid, sogar eine Gruppe dank $\iota: e \mapsto e$.

Aufgabe: Wie viele Verknüpfungen $*: \mathbb{Z}_2 \times \mathbb{Z}_2 \rightarrow \mathbb{Z}_2$ gibt es auf der Trägermenge $\mathbb{Z}_2 = \{0, 1\}$? Wie viele davon sind assoziativ? Wie viele Monoide $(G, *, e)$ gibt es? Wie viele Gruppen $(G, *, e, \iota)$? Welche kennen Sie bereits aus anderem Kontext? als Junktoren? Geben Sie diesen Verknüpfungen möglichst sprechende Namen.

Lösung: Die folgende Seite zeigt alle $2^{2 \times 2} = 16$ Möglichkeiten. Genau zwei davon sind Gruppen (grün), zwei weitere Monoide (gelb), und vier weitere immerhin noch assoziativ, also Halbgruppen (blau). Die verbleibenden acht (grau) sind nicht assoziativ. Übung!

Beispiele mit 0, 1 und 2 Elementen

c_0	0	1
0	0	0
1	0	0

$\bar{\vee}$	0	1
0	1	0
1	0	0

$<$	0	1
0	0	1
1	0	0

$\overline{\text{pr}}_1$	0	1
0	1	1
1	0	0

$>$	0	1
0	0	0
1	1	0

$\overline{\text{pr}}_2$	0	1
0	1	0
1	1	0

$\dot{\vee}$	0	1
0	0	1
1	1	0

$\bar{\wedge}$	0	1
0	1	1
1	1	0

\wedge	0	1
0	0	0
1	0	1

$=$	0	1
0	1	0
1	0	1

pr_2	0	1
0	0	1
1	0	1

\leq	0	1
0	1	1
1	0	1

pr_1	0	1
0	0	0
1	1	1

\geq	0	1
0	1	0
1	1	1

\vee	0	1
0	0	1
1	1	1

c_1	0	1
0	1	1
1	1	1

Beispiele mit 0, 1 und 2 Elementen

Die Mathematik lebt vom Wechselspiel zwischen konkret und abstrakt! Ein möglichst vielfältiger Beispielfundus ist wichtig zur Konkretisierung, um eindrucklich zu illustrieren und gegen naiven Irrglauben zu impfen.

Ich möchte Sie nachdrücklich zu guten Angewohnheiten ermutigen. Dazu gehört, auch einfache Fragen zu stellen und zu beantworten.

Bei jeder neuen Definition sollten Sie sich routinemäßig fragen:

Wie sehen mögliche Beispiele und Gegenbeispiele aus?

Wie hängen die Eigenschaften untereinander zusammen?

Impliziert eine die andere? Oder sind sie unabhängig?

Aufgabe: Gibt es Verknüpfungen, die kommutativ sind, aber nicht assoziativ? Wie sehen (kleinste) Beispiele aus?

Lösung: Schon mit unserem kleinen Beispielfundus ist dies leicht zu beantworten: Die kleinsten Beispiele gibt es bereits mit zwei Elementen, und hier finden wir genau zwei: $\overline{\vee}$ und $\overline{\wedge}$.

Assoziativität und Kommutativität

😊 In jeder Verknüpfungstabelle $* : M \times M \rightarrow M$ ist die Kommutativität leicht zu sehen als Spiegelsymmetrie entlang der Hauptdiagonalen.

😞 Die Assoziativität hingegen ist nicht offensichtlich, selbst in kleinen Beispielen wie diesen, und muss sorgsam nachgerechnet werden.

Führen Sie dies zur Übung an obigen Beispielen aus!

Neutrale Elemente: Eindeutigkeit

Beispiele: Gruppen: $(\mathbb{Z}, +, 0, -)$, $(\mathbb{Q}^*, \cdot, 1, -^1)$, $(GL_n \mathbb{R}, \cdot, 1_{n \times n}, -^1)$, $(S_n, \circ, \text{id}, -^1)$, ... Monoide: $(\mathbb{N}, +, 0)$, $(\mathbb{Z}, \cdot, 1)$, $(\mathbb{R}^{n \times n}, \cdot, 1_{n \times n})$, (E_n, \circ, id) , ... Halbgruppen: $(\mathbb{N}_{\geq 1}, +)$, $(2\mathbb{Z}, \cdot)$, ... Magmen: $(\mathbb{Z}, -)$, $(\mathfrak{P}(N), \setminus)$, ...

Lemma G1G: Links-/Rechts-/Neutrale und Eindeutigkeit

Sei $(M, *)$ ein Magma. Ein Element $e \in M$ heißt

- **linksneutral**, falls $e * a = a$ für alle $a \in M$ gilt,
- **rechtsneutral**, falls $a * e = a$ für alle $a \in M$ gilt,
- **(beidseitig) neutral**, falls beides gilt.

Ist $e \in G$ linksneutral und $e' \in G$ rechtsneutral, so folgt ihre Gleichheit:

$$e \stackrel{\text{rNr}}{=} e * e' \stackrel{\text{lNr}}{=} e'$$

In jedem Magma $(M, *)$ existiert höchstens ein neutrales Element!

Beispiele: In $(\mathbb{N}, +)$ ist 0 neutral. In $(\mathbb{N}_{\geq 1}, +)$ ist kein Element neutral. In $(\mathbb{Z}, -)$ ist das Nullelement 0 rechtsneutral, aber nicht linksneutral

Neutrale Elemente: Eindeutigkeit

😊 Gibt es Linksneutrale *und* Rechtsneutrale, so folgt Gleichheit. Das die Aussage von Lemma G1G, einfach aber bemerkenswert.

⚠️ Ohne Linksneutrales kann es mehrere Rechtsneutrale geben, und ohne Rechtsneutrales kann es mehrere Linksneutrale geben.

Beispiel: Wir betrachten nochmal die Verknüpfungen auf $\mathbb{Z}_2 = \{0, 1\}$, insbesondere die vier assoziativen, die kein neutrales Element haben:

c_0	0	1
0	0	0
1	0	0

c_1	0	1
0	1	1
1	1	1

pr_1	0	1
0	0	0
1	1	1

pr_2	0	1
0	0	1
1	0	1

Hier haben c_0 und c_1 weder Linksneutrales noch Rechtsneutrales, hingegen hat pr_1 zwei Rechtsneutrale, aber kein Linksneutrales, ebenso hat pr_2 zwei Linksneutrale, aber kein Rechtsneutrales.

😊 Diese Beispiele sind einfach doch konkret und hoffentlich hilfreich; Sie bezeugen, dass es in Lemma G1G wirklich etwas zu beweisen gibt! Diese Fragen und Bemerkungen illustrieren, wie wir umsichtig vorgehen und grundlegende Aussagen klären: durch Beweis oder Gegenbeispiel!

Lemma G1H: Links-/Rechts-/Inverse und Eindeutigkeit

Sei $(M, *, e)$ ein Monoid und $a, b, c \in M$.

Wir nennen b **linksinvers** zu a , falls $b * a = e$ gilt.

Wir nennen c **rechtsinvers** zu a , falls $a * c = e$ gilt.

Ist b linksinvers zu a und c rechtsinvers zu a , so folgt $b = c$, denn

$$b \stackrel{\text{rNtr}}{=} b * e \stackrel{\text{rInv}}{=} b * (a * c) \stackrel{\text{Ass}}{=} (b * a) * c \stackrel{\text{lInv}}{=} e * c \stackrel{\text{lNtr}}{=} c.$$

Wir nennen b **invers** zu a , falls sowohl $b * a = e$ als auch $a * b = e$ gilt.

Damit ist b eindeutig durch a bestimmt, und wir schreiben $a^{-1} := b$.

Die Menge aller invertierbaren Elemente in $(M, *, e)$ bezeichnen wir mit

$$M^\times = (M, *)^\times = (M, *, e)^\times := \{ a \in M \mid \exists b \in M : a * b = e = b * a \}.$$

Eindeutigkeit des Inversen zu a gilt immer, in jedem Monoid $(M, *, e)$;

Existenz muss gesondert gefordert werden: Das ist Axiom (G2).

Inverse Elemente: Eindeutigkeit

😊 Gibt es Linksinverse *und* Rechtsinverse, so folgt Gleichheit. Das die Aussage von Lemma G1H und durchaus bemerkenswert.

⚠️ Ohne Linksinverse kann es mehrere Rechtsinverse geben, und ohne Rechtsinverse kann es mehrere Linksinverse geben.

Beispiel: Wir betrachten das Monoid (M, \circ, id) aller Abbildungen $M = \{ f : \mathbb{N} \rightarrow \mathbb{N} \}$ mit Komposition \circ und neutralem Element $\text{id} = \text{id}_{\mathbb{N}}$. Die Abbildung $a : \mathbb{N} \rightarrow \mathbb{N} : n \mapsto n + 1$ ist injektiv und hat unendlich viele Linksinverse b_k für $k \in \mathbb{N}$, nämlich $b_k(0) = k$ und $b_k(n) = n - 1$ für $n \geq 1$. Jede Abbildung b_k ist surjektiv und hat zwei Rechtsinverse, nämlich neben a noch a_k mit $a_k(k) = 0$ und $a_k(n) = n + 1$ für alle $n \neq k$. Tatsächlich gilt $b_k \circ a = b_k \circ a_k = \text{id}_{\mathbb{N}}$, wie Sie sofort nachprüfen.

😊 Diese Beispiele sind einfach doch konkret und hoffentlich hilfreich; Sie bezeugen, dass es in Lemma G1H wirklich etwas zu beweisen gibt! Diese Fragen und Bemerkungen illustrieren, wie wir umsichtig vorgehen und grundlegende Aussagen klären: durch Beweis oder Gegenbeispiel!

Definition G11: Monoid und Gruppe, implizite Formulierung

Ein **Magma** $(G, *)$ ist eine Menge G mit Verknüpfung $* : G \times G \rightarrow G$.

(G0) Eine **Halbgruppe** $(G, *)$ erfüllt zudem die Assoziativität:

$$\mathbf{Ass}(G, *) \quad :\Leftrightarrow \quad \forall a, b, c \in G : (a * b) * c = a * (b * c)$$

(G1) Ein **Monoid** $(G, *)$ besitzt zudem ein neutrales Element:

$$\begin{aligned} \mathbf{Mon}(G, *) \quad &:\Leftrightarrow \quad \exists e \in G : \mathbf{Mon}(G, *, e) \\ &\Leftrightarrow \quad \begin{cases} \forall a, b, c \in G : (a * b) * c = a * (b * c) \\ \exists e \in G \quad \forall a \in G : e * a = a = a * e \end{cases} \end{aligned}$$

(G2) Eine **Gruppe** $(G, *, e)$ bzw. $(G, *)$ besitzt zudem eine Inversion:

$$\mathbf{Grp}(G, *, e) \quad :\Leftrightarrow \quad \exists(\iota : G \rightarrow G) : \mathbf{Grp}(G, *, e, \iota)$$

$$\begin{aligned} \mathbf{Grp}(G, *) \quad &:\Leftrightarrow \quad \exists e \in G \quad \exists(\iota : G \rightarrow G) : \mathbf{Grp}(G, *, e, \iota) \\ &\Leftrightarrow \quad \begin{cases} \forall a, b, c \in G : (a * b) * c = a * (b * c) \\ \exists e \in G \quad \forall a \in G : [e * a = a = a * e \\ \quad \wedge \exists b \in G : a * b = e = b * a] \end{cases} \end{aligned}$$

Monoide und Gruppen: implizite Definition

Formal korrekt besteht jede Gruppe $\underline{G} = (G, *, e, \iota)$ aus vier Daten: eine Trägermenge G und hierauf eine Verknüpfung $*: G \times G \rightarrow G$, hierzu ein neutrales Element $e \in G$ und eine Inversion $\iota: G \rightarrow G$.

😊 Die längliche Notation gelingt auch kürzer und bequemer:
Aus den drei Gruppendaten $(G, *, e)$ lässt sich ι rekonstruieren.
Aus den zwei Gruppendaten $(G, *)$ lassen sich e und ι rekonstruieren.

Die fehlenden Daten werden dabei nicht mehr explizit mitgeliefert, sondern implizit nur ihre Existenz gefordert. (Eindeutigkeit gilt ohnehin.)

Alle drei Schreibweisen haben ihren Nutzen und ihre Berechtigung. Selbst wenn ich mich auf eine festlegen wollte, in der Literatur werden Ihnen auch die anderen begegnen. Ich stelle Ihnen daher alle drei vor und nutze die für die jeweilige Situation am besten geeignete Variante.

⚠️ Allein aus der Menge G hingegen lässt sich $*$ nicht rekonstruieren! Die zugrundeliegende Menge G nennen wir auch **Trägermenge**. Die Verknüpfung $*: G \times G \rightarrow G$ ist eine **zusätzliche Struktur**!

Monoide und Gruppen: explizite vs implizite Definition

explizit $(G, *, e, \iota)$:	implizit $(G, *, e)$ bzw. $(G, *)$:
$(\mathbb{Z}, +, 0, -)$, $(\mathbb{Q}^*, \cdot, 1, ^{-1})$, $(\text{GL}_n \mathbb{R}, \cdot, 1_{n \times n}, ^{-1})$, $(S_n, \circ, \text{id}, ^{-1})$	$(\mathbb{Z}, +)$, (\mathbb{Q}^*, \cdot) , $(\text{GL}_n \mathbb{R}, \cdot)$, (S_n, \circ)
<p>😊 Alle vier Gruppendaten werden explizit genannt.</p> <p>😞 Die Notation ist leider etwas länglich.</p>	<p>😞 Manche Gruppendaten müssen implizit ergänzt werden.</p> <p>😊 Die Notation ist kurz und bequem.</p>
<p>😊 Die explizite Definition nutzt nur Allquantoren.</p> <p>😊 Sie ist meist leicht und routiniert nachzuprüfen.</p>	<p>😞 Die implizite Definition mischt All- und Existenzquantoren.</p> <p>😞 Die Mischung verkompliziert manche Nachweise.</p>

Pars pro toto: Oft sagt man „die Gruppe G “, meint aber $\underline{G} = (G, *, e, \iota)$.

⚠️ Allein die Menge G genügt i.A. nicht zur Definition der Gruppe \underline{G} !
 Sender und Empfänger treffen also eine wohlwollende Übereinkunft:
 Alle fehlenden Daten müssen aus dem Kontext erschlossen werden.

Aufgabe: Manche Autoren formulieren die Gruppenaxiome wie folgt:

$$\text{Grp}(G, *) \quad :\iff \quad \begin{cases} (0) \quad \forall a, b, c \in G : (a * b) * c = a * (b * c) \\ (1) \quad \exists e \in G \quad \forall a \in G : e * a = a * e = a \\ (2) \quad \forall a \in G \quad \exists b \in G : a * b = b * a = e \end{cases}$$

Ist das „sinngemäß irgendwie richtig“? Wo sehen Sie Probleme?
Vergleichen Sie dies mit der obigen Formulierung in Definition G11.

Lösung: Die Bedingungen (0) und (1) sind unkritisch. Zur Formulierung von (2) benötigen wir ein zusätzliches Element $e \in G$. Dessen Existenz wurde zwar in (1) gefordert, aber es könnte mehrere geben, dann würde die Richtigkeit der Aussage (2) von einer willkürlichen Wahl abhängen.

In der hier gezeigten Formulierung muss man daher nach (1) zunächst die Eindeutigkeit klären. Dieser logisch nötige Einschub wird oft ausgelassen oder nachgereicht. Beides ist nicht ideal.

Linksgruppen und Rechtsgruppen sind Gruppen.

😊 Die linke oder rechte Hälfte der Gruppenaxiome genügt bereits:

Satz G1J: Linksgruppen und Rechtsgruppen sind Gruppen.

Eine **Linksgruppe** $(G, *, e, ')$ erfüllt:

(G0) Die Verknüpfung $*$: $G \times G \rightarrow G$ ist assoziativ:

$$\forall a, b, c \in G : (a * b) * c = a * (b * c)$$

(G1L) Das Element $e \in G$ ist linksneutral:

$$\forall a \in G : e * a = a$$

(G2L) Zu jedem Element $a \in G$ ist das Element $a' \in G$ linksinvers:

$$\forall a \in G : a' * a = e$$

Erfreulicherweise ist jede Linksgruppe $(G, *, e, ')$ bereits eine Gruppe:
Das Element a' ist rechtsinvers zu a , und e ist rechtsneutral.

Alles gilt sinngemäß genauso für jede **Rechtsgruppe** dank G1B.

Linksgruppen und Rechtsgruppen sind Gruppen.

MathematikerInnen pflegen **Denkökonomie**, soweit dies möglich ist: Definitionen sollten keine unnötigen / redundanten Axiome fordern. Sätze sollten keine unnötigen Voraussetzungen verlangen.

☹ Für den Beweiser / Hersteller ist der Satz dann im Allgemeinen schwieriger zu beweisen. Bestenfalls genügt kritische Durchsicht: Guter Stil verlangt, nicht verwendete Voraussetzungen zu löschen.

😊 Schwächere Voraussetzungen bedeuten einen stärkeren Satz! Für den Anwender / Abnehmer ist der stärkere Satz allgemeiner und leichter anzuwenden, da weniger Voraussetzungen zu prüfen sind.

Unsere Definition G1I des Gruppenbegriffs ist noch etwas redundant: Die geforderten Axiome können weiter gekürzt werden (auf 3 von 5).

😊 Der obige Satz G1J ist der erste und letzte Satz über Linksgruppen: Wir führen diesen Begriff hier nur lokal als praktische Bezeichnung ein. Der Satz garantiert, dass es keinen Unterschied gibt zwischen Gruppen und Linksgruppen und Rechtsgruppen. Das ist nützlich zu wissen. Wir sprechen daher im Folgenden nur von Gruppen.

Linksgruppen und Rechtsgruppen sind Gruppen.

Beweis: Vorgelegt sei $a \in G$. Dank (G2L) gilt

$$a' * a = e \quad \text{und} \quad a'' * a' = e.$$

(G2R) Wir zeigen, dass a' rechtsinvers zu a ist:

$$\begin{aligned} a * a' &\stackrel{(G1L)}{=} e * (a * a') \stackrel{(G2L)}{=} (a'' * a') * (a * a') \stackrel{(G0)}{=} a'' * (a' * (a * a')) \\ &\stackrel{(G0)}{=} a'' * ((a' * a) * a') \stackrel{(G2L)}{=} a'' * (e * a') \stackrel{(G1L)}{=} a'' * a' \stackrel{(G2L)}{=} e \end{aligned}$$

(G1R) Wir zeigen, dass e rechtsneutral zu a ist:

$$a * e \stackrel{(G2L)}{=} a * (a' * a) \stackrel{(G0)}{=} (a * a') * a \stackrel{(G2R)}{=} e * a \stackrel{(G1L)}{=} a$$

Somit ist $(G, *, e, ')$ eine Gruppe, wie behauptet. **QED**

😊 Der Beweis ist raffiniert, dabei sehr kurz und vollkommen elementar.

Als leichte Übung können Sie jeden Rechenschritt sorgsam nachprüfen:

Allein aus (G0) sowie (G1L) und (G2L) folgern wir (G2R) und (G1R).

Somit erfüllt $(G, *, e, ')$ die Definition G11 einer Gruppe. Das war's.

Linksgruppen und Rechtsgruppen sind Gruppen.

😊 Einen solchen Beweis selbst auszutüfteln ist anfangs schwierig, aber durchaus möglich: Machen Sie mit Stift und Papier ein paar Versuche! Nur so gewinnen Sie eigene Erfahrung, können die Schwierigkeiten des Beweises erahnen und lernen gut formulierte Beweise zu schätzen!

Das illustriert verschiedene Stufen mathematischen Könnens:

- 1 Sätze genau lesen, richtig verstehen und korrekt anwenden.
- 2 Beweise kritisch lesen, alle Argumente verstehen und prüfen.
- 3 Beweise zu gegebenen Aussagen selbst finden und ausführen.
- 4 Sätze und Beweise eigenständig formulieren und erarbeiten.

Übung zur Illustration: Beweisen Sie die folgende Äquivalenz.

Korollar G1κ: ein Linksinverses zum Linksinversen

Sei $(M, *, e)$ ein Monoid. Angenommen, zum Element $a \in M$ existiert ein Linksinverses $a' \in M$, also $a' * a = e$. Dann sind äquivalent:

- (1) Das Linksinverse a' zu a ist auch rechtsinvers, also $a * a' = e$.
- (2) Auch zu a' existiert ein Linksinverses $a'' \in M$, also $a'' * a' = e$.

In diesem Falle ist a' eindeutig durch a bestimmt und $a'' = a$.

Lösung von Gleichungen in Gruppen

In $(\mathbb{R}, +, 0, -)$ lösen Sie Gleichungen wie in der Schule gelernt.

$$x + 5 = 3 \xrightarrow{\text{addiere } -5} x = 3 + (-5)$$

In jeder Gruppe $(G, *, e, ')$ können Sie Gleichungen ebenso lösen!

$$x * a = b \xrightarrow{\text{multipliziere } a' \text{ von rechts}} x = b * a'$$

$$a * y = b \xrightarrow{\text{multipliziere } a' \text{ von links}} y = a' * b$$

Satz G1L: Lösung von Gleichungen in Gruppen

Gegeben sei eine nicht-leere Halbgruppe $(G, *)$, also eine Menge $G \neq \emptyset$ mit assoziativer Verknüpfung $* : G \times G \rightarrow G$. Dann sind äquivalent:

- (1) **Neutrales und Inverse:** Es existiert ein neutrales Element $e \in G$ und eine Inversion $' : G \rightarrow G$, die $(G, *, e, ')$ zu einer Gruppe machen.
- (2) **Lösbarkeit von Gleichungen:** Zu je zwei Elementen $a, b \in G$ existieren Lösungen $x, y \in G$ der Gleichungen $x * a = b$ und $a * y = b$.

Zusatz: Die Lösungen x, y sind dann eindeutig durch a, b bestimmt und dank Inversion explizit gegeben durch $x = b * a'$ und $y = a' * b$.

Lösung von Gleichungen in Gruppen

😊 Die Implikation „(1) \Rightarrow (2)“ betrifft das Lösen von Gleichungen: Dies werden Sie häufig für Rechnungen in Gruppen nutzen können. Sie ist sehr leicht zu beweisen, versuchen Sie es zunächst selbst!

Die Implikation „(2) \Rightarrow (1)“ zeigt umgekehrt, dass die Lösbarkeit von Gleichungen die Gruppenaxiome impliziert. Das ist bemerkenswert! Wir müssen dazu lediglich $G \neq \emptyset$ und Assoziativität voraussetzen.

Assoziativität wollen wir aus diversen Gründen immer voraussetzen. Die hier sorgsam ausformulierte Äquivalenz „(1) \Leftrightarrow (2)“ besagt also:

😊 Allgemeine Gleichungen der Form $a * x = b$ und $y * a = b$ können wir in Gruppen lösen – und nur in Gruppen!

Hier sehen wir eine weitere, hilfreiche Charakterisierung von Gruppen. Für das Lösen von Gleichungen benötigen wir genau diese Struktur!

😊 Bereits diese ersten einfachen Rechnungen und Ergebnisse deuten an, dass Gruppen eine grundlegende Struktur der Mathematik sind.

Lösung von Gleichungen in Gruppen

Beweis: „(1) \Rightarrow (2)“: $x = b * a'$ und $y = a' * b$ lösen die Gleichungen:

$$x * a = (b * a') * a \stackrel{(G0)}{=} b * (a' * a) \stackrel{(G2)}{=} b * e \stackrel{(G1)}{=} b$$

$$a * y = a * (a' * b) \stackrel{(G0)}{=} (a * a') * b \stackrel{(G2)}{=} e * b \stackrel{(G1)}{=} b$$

Umgekehrt: Aus $x * a = b$ bzw. $a * y = b$ folgt:

$$x \stackrel{(G1)}{=} x * e \stackrel{(G2)}{=} x * (a * a') \stackrel{(G0)}{=} (x * a) * a' \stackrel{!}{=} b * a'$$

$$y \stackrel{(G1)}{=} e * y \stackrel{(G2)}{=} (a' * a) * y \stackrel{(G0)}{=} a' * (a * y) \stackrel{!}{=} a' * b$$

„(2) \Rightarrow (1)“: Wir zeigen die Eigenschaften (G1L) und (G2L).

(G1L) Wir wählen $a \in G$. Hierzu existiert ein Element $e \in G$ mit $e * a = a$.
Zu jedem Element $b \in G$ existiert ein $y \in G$ mit $a * y = b$. Daraus folgt:

$$e * b = e * (a * y) \stackrel{(G0)}{=} (e * a) * y \stackrel{(G1)}{=} a * y = b$$

Also ist e linksneutral. (G2L) Zu $a \in G$ existiert $a' \in G$ mit $a' * a = e$.

Somit ist $(G, *, e, ')$ eine Linksgruppe, dank G1J also eine Gruppe. QED

Lösung von Gleichungen in Gruppen

- 😊 Auch dieser Beweis ist recht raffiniert, dabei kurz und elementar. Ich führe dies exemplarisch aus, damit Sie an diesem Vorbild lernen. Zur besseren Übersicht haben wir die Argumente geschickt aufgebaut: Zunächst beweisen wir, dass Linksgruppen stets Gruppen sind (G1J). Dies nutzen wir dankend im obigen Beweis von Satz G1L, da wir nun nur noch die Hälfte der Gruppenaxiome prüfen müssen. Ich betone: MathematikerInnen pflegen Denkökonomie, soweit dies möglich ist: Definitionen sollten keine unnötigen / redundanten Axiome fordern.
- 😊 Hier sehen Sie recht eindrücklich die beiden Seiten der Medaille. Für den Beweiser / Hersteller ist der stärkere Satz meist schwieriger zu beweisen. Für den Anwender / Abnehmer jedoch ist der stärkere Satz leichter anzuwenden. Oft stehen Sie (abwechselnd) auf beiden Seiten. Als Anwender mathematischer Ergebnisse schätzen Sie die Garantie. Als Hersteller mathematischer Ergebnisse spüren Sie die Pflicht. Wie bereits in Kapitel C zur Induktion gilt das Grundprinzip: Ihre Vorbereitung von heute ist Ihr Nutzen von morgen!

Sudoku als Verknüpfungstabelle

2	5			3		9		1
	1				4			
4		7				2		8
		5	2					
				9	8	1		
	4				3			
			3	6			7	2
	7							3
9		3				6		4

Lösung
→

2	5	8	7	3	6	9	4	1
6	1	9	8	2	4	3	5	7
4	3	7	9	1	5	2	6	8
3	9	5	2	7	1	4	8	6
7	6	2	4	9	8	1	3	5
8	4	1	6	5	3	7	2	9
1	8	4	3	6	9	5	7	2
5	7	6	1	4	2	8	9	3
9	2	3	5	8	7	6	1	4

	2			3		9		7
	1							
4		7				2		8
		5	2				9	
			1	8		7		
	4				3			
				6			7	1
	7							
9		3		2		6		5

Lösung
→

6	2	8	5	3	4	9	1	7
5	1	9	8	7	2	4	3	6
4	3	7	9	1	6	2	5	8
8	6	5	2	4	7	1	9	3
3	9	2	1	8	5	7	6	4
7	4	1	6	9	3	5	8	2
2	5	4	3	6	9	8	7	1
1	7	6	4	5	8	3	2	9
9	8	3	7	2	1	6	4	5

Aufgabe: Ist jede Gleichung $a * x = b$ und $y * a = b$ eindeutig lösbar?
Gibt es kommutative Sudokus? und assoziative Sudokus? Satz G1L!

Sudoku als Verknüpfungstabelle

Lösung: Die Sudoku-Regeln verlangen, dass in jeder vollständig gelösten Tabelle jede der Zahlen $1, \dots, 9$ genau einmal vorkommt

- 1 in jeder der neun Zeilen und
- 2 in jeder der neun Spalten sowie
- 3 in jedem der neun Teilquadrate.

Wir betrachten die Menge $G = \{1, \dots, 9\}$ mit Tabelle $*$: $G \times G \rightarrow G$.

Bedingung (1) bedeutet: Für alle $a, b \in G$ ist $a * x = b$ eindeutig lösbar.

Bedingung (2) bedeutet: Für alle $a, b \in G$ ist $y * a = b$ eindeutig lösbar.

(a) Kommutativität verletzt Bedingung (3) und ist daher ausgeschlossen.

(b) Aus den Bedingungen (1) und (2) und Assoziativität folgt dank G1L, dass $(G, *)$ eine Gruppe ist. Insbesondere existiert dann ein neutrales Element $e \in G$. Ist $e = 1$, so haben wir $1 * 2 = 2 * 1$, was (3) widerspricht.

Allgemein sei $g \in G$ ein Nachbar von e in der selben Dreiergruppe.

Dann gilt $e * g = g * e$, also ist Bedingung (3) auch hier verletzt.

Wir schließen: Es gibt keine assoziativen Sudokus!

Quasigruppen und Sudoku

Eine **Quasigruppe** $(G, *)$ ist eine Menge G mit einer Verknüpfung $*: G \times G \rightarrow G$ und folgender Lösbarkeitseigenschaft:

Zu je zwei Elementen $a, b \in G$ existieren eindeutige Lösungen $x, y \in G$ der Gleichungen $x * a = b$ und $a * y = b$.

Zusammen mit Assoziativität erhalten wir eine Gruppe, siehe G1L:
Jede assoziative Quasigruppe ist eine Gruppe.

Die obigen Sudokus zeigen weitere Beispiele von Quasigruppen.
Zu einer Gruppe fehlt allein die Assoziativität.

Gruppen und Assoku

Viele Menschen weltweit lieben Sudokus und betreiben leidenschaftlich quasi Gruppentheorie als Hobby, als Zeitvertreib oder als Gehirnjogging. Ein besonderer Reiz an Quasigruppen ist, dass es davon sehr viele gibt und daher der Rätselspaß anscheinend niemals langweilig wird.

Gruppen sind besonders stark strukturiert und daher für dieses Rätsel zu einfach. Es gibt bis auf Isomorphie (also Umordnung der Elemente) genau zwei Gruppen mit neun Elementen, nämlich $\mathbb{Z}/9$ und $\mathbb{Z}/3 \times \mathbb{Z}/3$. Mit diesem Wissen ist jedes Gruppen-Sudoku viel leichter zu lösen.

Dennoch wäre dies eine bemerkenswerte Variante. Probieren Sie es! Ich schlage hierzu den Namen „Assoku“ vor: assoziatives Sudoku, die Regel der neun Teilquadrate wird durch Assoziativität ersetzt. Das Spielvergnügen kann man nur experimentell ermitteln.

Linkstranslationen

Sei $(G, *)$ ein Magma, also eine Menge G mit $* : G \times G \rightarrow G$.
Zu jedem Element $a \in G$ betrachten wir seine Linkstranslation

$$\lambda_a : G \rightarrow G : x \mapsto a * x.$$

Dies klärt die Lösungen von Gleichungen der Form $a * x = b$:

- Ist λ_a surjektiv, so nennen wir a **linkslösbar**:
Zu jedem $b \in G$ existiert $x \in G$ mit $a * x = b$.
- Ist λ_a injektiv, so nennen wir a **linkskürzbar**:
Für alle $x, y \in G$ gilt: Aus $a * x = a * y$ folgt $x = y$.
- Ist λ_a bijektiv, so nennen wir a **linksdividierbar**.
Wir definieren die Linksdivision durch $a \setminus b = \lambda_a^{-1}(b)$.

Entsprechend für die Rechtstranslation

$$\rho_a : G \rightarrow G : x \mapsto x * a.$$

Dies klärt die Lösungen von Gleichungen der Form $x * a = b$:

- Ist ρ_a surjektiv, so nennen wir a **rechtslösbar**:
Zu jedem $b \in G$ existiert $x \in G$ mit $x * a = b$.
- Ist ρ_a injektiv, so nennen wir a **rechtskürzbar**:
Für alle $x, y \in G$ gilt: Aus $x * a = y * a$ folgt $x = y$.
- Ist ρ_a bijektiv, so nennen wir a **rechtsdividierbar**.
Wir definieren die Rechtsdivision durch $b/a = \rho_a^{-1}(b)$.

Beispiel: Ist $(G, *, e, {}^{-1})$ eine Gruppe, so ist jedes Element $a \in G$ sowohl linksdividierbar dank $a \setminus b = a^{-1} * b$ als auch rechtsdividierbar dank $b / a = b * a^{-1}$. Genau dies nutzen wir zur Lösung von Gleichungen!

Beispiel: Satz G1L besagt: Ist $(G, *)$ assoziativ und jedes Element $a \in G$ sowohl links- als auch rechtlösbar, so ist $(G, *)$ eine Gruppe.

Beispiel: In einer Quasigruppe $(Q, *)$ ist jedes Element linksdividierbar und rechtsdividierbar. Die obigen Sudokus illustrieren dies durch Beispiele ohne neutrales Element und ohne Assoziativität.

Lösbar und kürzbar impliziert invertierbar.

Aufgabe: Sei $(M, *, 1)$ ein Monoid und $a \in M$ ein Element.

(1) Ist a linkslösbar und linkskürzbar, so ist a invertierbar.

(2) Ist a rechtslösbar und rechtskürzbar, so ist a invertierbar.

Lösung: (1) Nach Voraussetzung ist $\lambda_a : M \rightarrow M : x \mapsto ax$ surjektiv.

Also existiert $b \in M$ mit $ab = 1$, das heißt, a ist rechtsinvertierbar.

Zudem ist $\lambda_a : M \rightarrow M : x \mapsto ax$ injektiv, also a linkskürzbar.

Wir haben $a1 = a = 1a = (ab)a = a(ba)$, nach Kürzen also $1 = ba$.

Demnach ist das Element a invertierbar durch b , denn $ab = 1 = ba$.

(2) Diese Aussage beweist man wörtlich genauso wie (1) durch Vertauschen von links und rechts, also Übergang zu $(M, *^{\text{op}}, 1)$.

Unterstrukturen durch Einschränkung

Sei $(G, *)$ ein Magma, also eine Menge mit Verknüpfung $* : G \times G \rightarrow G$.

Für jede Teilmenge $U \subseteq G$ können wir die Verknüpfung einschränken zu

- $*|_{U \times G} : U \times G \rightarrow G : (u, a) \mapsto u * a$ Linksoperation von U auf G ,
- $*|_{G \times U} : G \times U \rightarrow G : (a, u) \mapsto a * u$ Rechtsoperation von U auf G ,
- $*|_{U \times U} : U \times U \rightarrow G : (u, v) \mapsto u * v$ äußere Verknüpfung auf U .

Diese drei Einschränkungen gelingen immer und sind oft nützlich.

Für ganz besondere Teilmengen $U \subseteq G$ erhalten wir die Einschränkung

$$*_U = *|_{U \times U}^U : U \times U \rightarrow U : (u, v) \mapsto u * v.$$

Dies gelingt nicht immer, sondern erfordert die **Abgeschlossenheit** der Teilmenge $U \subseteq G$ unter der Verknüpfung $* : G \times G \rightarrow G$, also:

$$U * U \subseteq U \iff \forall a, b \in U : a * b \in U$$

In Worten: Wenn wir zwei Elemente a, b aus U mit $*$ verknüpfen, dann erhalten wir immer ein Element $a * b$ in U (und nicht bloß irgendwo in G).

Unterstrukturen durch Einschränkung

Definition G1M: Unterstrukturen durch Einschränkung

Sei $(G, *)$ ein Magma, also $*: G \times G \rightarrow G$. Ein **Untermagma** $U \leq (G, *)$ ist eine Teilmenge $U \subseteq G$ mit $U * U \subseteq U$. Ausführlich: Für alle $a, b \in U$ gilt $a * b \in U$. Somit ist die Einschränkung $*_U = *|_{U \times U}: U \times U \rightarrow U$ von $*$ auf U wohldefiniert, und $(U, *_U)$ ist selbst ein Magma.

(G0) Ist $(G, *)$ assoziativ bzw. kommutativ, so auch $(U, *_U)$.

(G1) Für ein **Untermonoid** $U \leq (G, *, e)$ fordern wir zudem $e \in U$. Somit ist $(U, *_U, e)$ ein Monoid, denn $e * a = a * e = a$ für alle $a \in U$.

Ist $(U, *_U, e)$ zudem eine Gruppe, so nennen wir U eine **Untergruppe** im Monoid $(G, *, e)$. Ist $(G, *, e, \iota)$ selbst eine Gruppe, so bedeutet das:

(G2) Für eine **Untergruppe** $U \leq (G, *, e, \iota)$ fordern wir zudem $\iota(U) \subseteq U$. Ausführlich: Für alle $a \in U$ gilt $\iota(a) \in U$. Somit ist die Einschränkung $\iota_U = \iota|_U: U \rightarrow U$ wohldefiniert, und $(U, *_U, e, \iota_U)$ ist eine Gruppe.

Untergruppen

Beispiel: In jeder Gruppe $(G, *, e, \iota)$ sind $\{e\}$ und G Untergruppen.

Beispiele: In der Gruppe $(\mathbb{Z}, +, 0, -)$ gilt:

- Die Menge $2\mathbb{Z}$ ist eine Untergruppe, aber nicht $2\mathbb{Z} + 1$.
- Die Menge $U = n\mathbb{Z}$ mit $n \in \mathbb{N}$ ist eine Untergruppe. Umgekehrt:
- Jede Untergruppe $U < \mathbb{Z}$ hat die Form $U = n\mathbb{Z}$, siehe Satz G1v.
- Die Menge \mathbb{N} ist ein Untermonoid, aber keine Untergruppe.
- Die Menge $\mathbb{N}_{\geq 5}$ ist eine Unterhalbgruppe, aber kein Untermonoid.

Beispiel: Im Monoid $(\mathbb{Z}, \cdot, 1)$ ist $\{0\}$ multiplikativ abgeschlossen, und $(\{0\}, \cdot, 0)$ ist ein Monoid, aber kein Untermonoid von $(\mathbb{Z}, \cdot, 1)$.

Übung: In der symmetrischen Gruppe S_3 gibt es genau 6 Untergruppen.

Aufgabe: Die Untergruppenbedingung lässt sich wie folgt formulieren:

$$\begin{aligned}
 U \leq (G, *, e, \iota) & \quad :\iff e \in U \wedge \forall a, b \in U : [a * b \in U \wedge \iota(a) \in U] \\
 & \quad \iff U \neq \emptyset \wedge \forall a, b \in U : a * \iota(b) \in U
 \end{aligned}$$

Lösung: Die Implikation „ \Rightarrow “ ist klar. Wir zeigen „ \Leftarrow “:

(0) Wegen $U \neq \emptyset$ existiert $a \in U$, somit $e = a * \iota(a) \in U$.

(1) Für jedes $a \in U$ gilt dank (0) auch $\iota(a) = e * \iota(a) \in U$.

(2) Für alle $a, b \in U$ gilt $\iota(b) \in U$ dank (1), also $a * b = a * \iota(\iota(b)) \in U$.

Notation: Für eine Untergruppe $U \subseteq G$ in $(G, *)$ schreiben wir kurz $U \leq (G, *)$ oder noch kürzer $U \leq G$. Im Falle $U \subsetneq G$ ist U eine **echte Untergruppe**, geschrieben $U < G$. Dieselbe Notation nutzen wir für Untermonoide; der Kontext macht jeweils klar, was gemeint ist.

Die invertierbaren Elemente bilden eine Untergruppe.

Beispiele: Im Matrixring $K^{n \times n}$ gilt $(K^{n \times n}, \cdot, 1_{n \times n})^\times = \text{GL}_n K$.

Im Monoid $(E_X, \circ, \text{id}_X)$ mit $E_X = \text{Abb}(X, X)$ gilt $E_X^\times = S_X$.

Im Ring \mathbb{Z}_n gilt $\mathbb{Z}_n^\times = (\mathbb{Z}_n, \cdot, 1)^\times = \{ a \in \mathbb{Z}_n \mid \text{ggT}(a, n) = 1 \}$.

Ein Monoid $(M, *, e)$ ist genau dann eine Gruppe, wenn $M^\times = M$ gilt.

Satz G1N: Die invertierbaren Elemente bilden eine Gruppe.

In jedem Monoid $(M, *, e)$ ist $M^\times \leq (M, *, e)$ eine Untergruppe.

In M^\times gilt $e^{-1} = e$ und $(a^{-1})^{-1} = a$ sowie $(a * b)^{-1} = b^{-1} * a^{-1}$.

Übung: Beweisen Sie dies zur Wiederholung (B1c).

Die invertierbaren Elemente bilden eine Untergruppe.

Beweis: Zunächst gilt $e * e = e$, also $e \in M^\times$ mit $e^{-1} = e$.

Für je zwei Elemente $a, b \in M^\times$ gilt $a * b \in M^\times$, denn wir haben:

$$(a * b) * (b^{-1} * a^{-1}) \stackrel{\text{Ass}}{=} (a * (b * b^{-1})) * a^{-1} \stackrel{\text{Inv}}{=} (a * 1) * a^{-1} \stackrel{\text{Ntr}}{=} a * a^{-1} \stackrel{\text{Inv}}{=} e$$

$$(b^{-1} * a^{-1}) * (a * b) \stackrel{\text{Ass}}{=} (b^{-1} * (a^{-1} * a)) * b \stackrel{\text{Inv}}{=} (b^{-1} * 1) * b \stackrel{\text{Ntr}}{=} b^{-1} * b \stackrel{\text{Inv}}{=} e$$

Also ist $a * b$ invertierbar mit dem Inversen $(a * b)^{-1} = b^{-1} * a^{-1}$.

Das heißt, M^\times enthält e und ist abgeschlossen unter Multiplikation.

Für $a \in M^\times$ gilt $a * a^{-1} = a^{-1} * a = e$, also $a^{-1} \in M^\times$ mit $(a^{-1})^{-1} = a$.

Somit ist die Inversion $^{-1} : M^\times \rightarrow M^\times : a \mapsto a^{-1}$ auf M^\times wohldefiniert.

Zusammengefasst bedeutet das: $(M^\times, *, e, ^{-1})$ ist eine Gruppe. QED

Beispiele zu Untergruppen

- Übung:** (1) Ist $(U_i)_{i \in I}$ eine Familie von Untergruppen $U_i \leq (G, *, e, \iota)$, so ist auch die Schnittmenge $U = \bigcap_{i \in I} U_i$ eine Untergruppe in G .
- (2) Geben Sie ein Beispiel für zwei Untergruppen $U, V \leq (G, *, e, \iota)$, sodass ihre Vereinigung $U \cup V$ keine Untergruppe in G ist.

Beispiele zu Untergruppen

Zu jedem Monoid (G, \cdot, e) definieren wir das **Zentrum** als die Menge

$$Z(G) = Z(G, \cdot) = \{ z \in G \mid \forall a \in G : a \cdot z = z \cdot a \}$$

aller Elemente $z \in G$, die mit allen Elementen in G kommutieren.

- Übung:** (1) Das Zentrum $Z(G)$ ist ein Untermonoid von (G, \cdot, e) .
(2) Ist ein Element $z \in Z(G)$ invertierbar in G , so gilt $z^{-1} \in Z(G)$.
(3) Ist $(G, *, e)$ eine Gruppe, so ist $Z(G)$ eine Untergruppe.
(4) Allgemein gilt $Z(G)^\times = Z(G) \cap G^\times$.

Homomorphismen sind strukturerhaltende Abbildungen.

Die Exponentialfunktion $\exp : \mathbb{R} \rightarrow \mathbb{R}_{>0} : a \mapsto e^a = \sum_{k=0}^{\infty} a^k / k!$ erfüllt $\exp(a + b) = \exp(a) \cdot \exp(b)$ sowie $\exp(0) = 1$ und $\exp(-x) = \exp(x)^{-1}$.

$$\begin{array}{ccc}
 \mathbb{R} \times \mathbb{R} & \xrightarrow[\quad (a,b) \mapsto a+b \quad]{+} & \mathbb{R} \\
 \exp \downarrow & & \exp \downarrow \\
 \mathbb{R}_{>0} \times \mathbb{R}_{>0} & \xrightarrow[\quad (x,y) \mapsto x \cdot y \quad]{\cdot} & \mathbb{R}_{>0}
 \end{array}
 \qquad
 \begin{array}{ccc}
 0 & & \\
 \exp \downarrow & & \\
 1 & &
 \end{array}
 \qquad
 \begin{array}{ccc}
 \mathbb{R} & \xrightarrow[\quad a \mapsto -a \quad]{-} & \mathbb{R} \\
 \exp \downarrow & & \exp \downarrow \\
 \mathbb{R}_{>0} & \xrightarrow[\quad x \mapsto x^{-1} \quad]{-1} & \mathbb{R}_{>0}
 \end{array}$$

Die Logarithmusfunktion $\ln : \mathbb{R}_{>0} \rightarrow \mathbb{R}$ erfüllt $\ln(x \cdot y) = \ln(x) + \ln(y)$ sowie $\ln(1) = 0$ und $\ln(x^{-1}) = -\ln(x)$. Übersichtlich als Diagramm:

$$\begin{array}{ccc}
 \mathbb{R}_{>0} \times \mathbb{R}_{>0} & \xrightarrow[\quad (x,y) \mapsto x \cdot y \quad]{\cdot} & \mathbb{R}_{>0} \\
 \ln \downarrow & & \ln \downarrow \\
 \mathbb{R} \times \mathbb{R} & \xrightarrow[\quad (a,b) \mapsto a+b \quad]{+} & \mathbb{R}
 \end{array}
 \qquad
 \begin{array}{ccc}
 1 & & \\
 \ln \downarrow & & \\
 0 & &
 \end{array}
 \qquad
 \begin{array}{ccc}
 \mathbb{R}_{>0} & \xrightarrow[\quad x \mapsto x^{-1} \quad]{-1} & \mathbb{R}_{>0} \\
 \ln \downarrow & & \ln \downarrow \\
 \mathbb{R} & \xrightarrow[\quad a \mapsto -a \quad]{-} & \mathbb{R}
 \end{array}$$

Homomorphismen sind strukturerhaltende Abbildungen.

Ein Homomorphismus ist eine strukturerhaltende Abbildung.

Wir erklären hier, was das genau bedeutet. Es lohnt sich, dies für jede mathematische Struktur zu definieren, zu untersuchen und zu nutzen.

Sie kennen und nutzen Homomorphismen bereits seit Schulzeiten, wenn auch nicht unter diesem Namen, meist unter gar keinem Namen.

Viele nützliche Rechenregeln, wie Potenzgesetze, Exponentialgesetze, Logarithmusgesetze und zahllose weitere, sind letztendlich nichts weiter als Homomorphismen (oder beruhen darauf). Wir wollen dies bündeln.

Die obigen Beispiele $\exp: (\mathbb{R}, +) \rightarrow (\mathbb{R}_{>0}, \cdot)$ und $\ln: (\mathbb{R}_{>0}, \cdot) \rightarrow (\mathbb{R}, +)$ sind Gruppenhomomorphismen, allgemein ist dies eine Abbildung

$f: (G, *, e_G, \iota_G) \rightarrow (H, \cdot, e_H, \iota_H)$ mit folgenden Eigenschaften:

$$\begin{array}{ccccc}
 G \times G & \xrightarrow[\quad (a,b) \mapsto a*b \quad]{*} & G & e_G \in G & G \xrightarrow[\quad a \mapsto \iota_G(a) \quad]{\iota_G} & G \\
 \downarrow f & & \downarrow f & \downarrow f & \downarrow f & \downarrow f \\
 H \times H & \xrightarrow[\quad (x,y) \mapsto x \cdot y \quad]{\cdot} & H & e_H \in H & H \xrightarrow[\quad x \mapsto \iota_H(x) \quad]{\iota_H} & H
 \end{array}$$

Homomorphismen sind strukturerhaltende Abbildungen.

Definition G10: Homomorphismen

Ein **Homomorphismus** ist eine strukturerhaltende Abbildung.

(G0) Für Magmen und Halbgruppen verlangen wir Multiplikativität:

$$\left. \begin{array}{l} f : (G, *) \rightarrow (H, \cdot) \\ \text{Magmahomomorphismus} \end{array} \right\} \iff \left\{ \begin{array}{l} f : G \rightarrow H \text{ Abbildung und} \\ \forall a, b \in G : f(a * b) = f(a) \cdot f(b) \end{array} \right.$$

(G1) Für einen **Monoidhomomorphismus** fordern wir zudem $f(e) = e'$:

$$\left. \begin{array}{l} f : (G, *, e) \rightarrow (H, \cdot, e') \\ \text{Monoidhomomorphismus} \end{array} \right\} \iff \left\{ \begin{array}{l} f : G \rightarrow H \text{ mit } f(e) = e' \text{ und} \\ \forall a, b \in G : f(a * b) = f(a) \cdot f(b) \end{array} \right.$$

(G2) Für einen **Gruppenhomomorphismus** genügt Multiplikativität:

$$\left. \begin{array}{l} f : (G, *, e, \iota) \rightarrow (H, \cdot, e', \iota') \\ \text{Gruppenhomomorphismus} \end{array} \right\} \iff \left\{ \begin{array}{l} f : G \rightarrow H \text{ Abbildung und} \\ \forall a, b \in G : f(a * b) = f(a) \cdot f(b) \end{array} \right.$$

Daraus folgt bereits $f(e) = e'$ und $f \circ \iota = \iota' \circ f$, also $f(a^{-1}) = f(a)^{-1}$.

Homomorphismen sind strukturerhaltende Abbildungen.

Beispiel: Die Abbildung $f : (\mathbb{N}, \cdot, 1) \rightarrow (\mathbb{Z}, \cdot, 1) : a \mapsto 0$ ist multiplikativ, $f(a \cdot b) = f(a) \cdot f(b)$, aber kein Monoidhomomorphismus: $f(1) = 0 \neq 1$.

Schreibweise für Gruppenhomomorphismen:

$$\begin{aligned} \text{Hom}(G, H) &= \text{Hom}(G, *, H, \cdot) = \text{Hom}(G, *, e, \iota; H, \cdot, e', \iota') \\ &:= \{ f : G \rightarrow H \mid \forall a, b \in G : f(a * b) = f(a) \cdot f(b) \} \end{aligned}$$

Aufgabe: Folgern Sie $f(e) = e'$ und $f(a^{-1}) = f(a)^{-1}$.

Lösung: (1) Wir betrachten

$$e' \cdot f(e) \stackrel{\text{Ntr}}{=} f(e) \stackrel{\text{Ntr}}{=} f(e * e) \stackrel{\text{Hom}}{=} f(e) \cdot f(e).$$

Multiplikation mit $f(e)^{-1}$ von rechts ergibt $e' = f(e)$.

(2) Für jedes Element $a \in G$ gilt

$$e' \stackrel{(1)}{=} f(e) \stackrel{\text{Inv}}{=} f(a * a^{-1}) \stackrel{\text{Hom}}{=} f(a) \cdot f(a^{-1}).$$

Wir folgern $f(a^{-1}) = f(a)^{-1}$ dank Eindeutigkeit des Inversen (G1H).

Isomorphismen sind strukturerhaltende Bijektionen.

Ist $\varphi: (G, *) \rightarrow (H, \cdot)$ ein Homomorphismus und zudem bijektiv, so nennen wir f einen **Isomorphismus** von $(G, *)$ nach (H, \cdot) .

Lemma G1P: Umkehrung eines Isomorphismus

In diesem Falle ist auch $\psi = \varphi^{-1}: (H, \cdot) \rightarrow (G, *)$ ein Isomorphismus.

Beweis: Zu $x, y \in H$ sei $a = \psi(x)$ und $b = \psi(y)$. Damit folgt:
 $\psi(x \cdot y) = \psi(\varphi(a) \cdot \varphi(b)) = \psi(\varphi(a * b)) = a * b = \psi(x) * \psi(y)$. □

Definition G1Q: Isomorphismus als Paar

Ein **Isomorphismus** $(\varphi, \psi): (G, *) \cong (H, \cdot)$ zwischen zwei Gruppen ist ein Paar zueinander inverser Homomorphismen $\varphi: (G, *) \rightarrow (H, \cdot)$ und $\psi: (H, \cdot) \rightarrow (G, *)$ mit $\psi \circ \varphi = \text{id}_G$ und $\varphi \circ \psi = \text{id}_H$.

Entsprechend für $(\varphi, \psi): (G, *, e) \cong (H, \cdot, e')$ zwischen zwei Monoiden. (Es genügt, einen anzugeben, der andere ist dann eindeutig bestimmt. Es ist jedoch oft bequem, das Paar vollständig und explizit anzugeben.)

Beispiel: Wir haben $(\exp, \ln): (\mathbb{R}, +) \cong (\mathbb{R}_{>0}, \cdot)$.

Isomorphismen sind strukturerhaltende Bijektionen.

Schreibweise für **Homomorphismen** und **Isomorphismen**:

$$\text{Hom}(G, *; H, \cdot) = \{ f : G \rightarrow H \mid \forall a, b \in G : f(a * b) = f(a) \cdot f(b) \}$$

$$\text{Iso}(G, *; H, \cdot) = \{ f : G \xrightarrow{\sim} H \mid \forall a, b \in G : f(a * b) = f(a) \cdot f(b) \}$$

Im Spezialfall $(G, *) = (H, \cdot)$ stimmen Start und Ziel überein, und wir sprechen dann von **Endomorphismen** und **Automorphismen**:

$$\text{End}(G, *) = \text{Hom}(G, *; G, *)$$

$$\text{Aut}(G, *) = \text{Iso}(G, *; G, *)$$

Beispiel: Für $f : \mathbb{R}_{>0} \rightarrow \mathbb{R}_{>0} : x \mapsto x^n$ mit $n \in \mathbb{N}_{\geq 1}$ gilt $f \in \text{Aut}(\mathbb{R}_{>0}, \cdot)$.

Es gilt $f(x \cdot y) = (x \cdot y)^n = x^n \cdot y^n = f(x) \cdot f(y)$, also $f \in \text{End}(\mathbb{R}_{>0}, \cdot)$.

Zudem ist f invertierbar, durch $g(y) = \sqrt[n]{y}$, also gilt $f \in \text{Aut}(\mathbb{R}_{>0}, \cdot)$.

Bemerkung: Dank G1P folgt daraus $\sqrt[n]{x \cdot y} = \sqrt[n]{x} \cdot \sqrt[n]{y}$.

L'algèbre est généreuse, elle donne souvent plus qu'on lui demande.

[Die Algebra ist großzügig, sie gibt oft mehr, als wir von ihr verlangen.]

Jean Le Rond d'Alembert (1717–1783)

Homomorphismen und Untergruppen

Satz G1R: Bild und Kern, surjektiv und injektiv

Sei $f: (G, *, e) \rightarrow (H, \cdot, e')$ ein Gruppenhomomorphismus.

(1) Ist $U \leq (G, *, e)$ eine Untergruppe, so auch $V = f(U) \leq (H, \cdot, e')$. Insbesondere ist das Bild $\text{im}(f) = f(G) \leq (H, \cdot, e')$ eine Untergruppe.

(2) Genau dann ist f surjektiv, wenn $\text{im}(f) = H$ gilt.

(3) Ist $V \leq (H, \cdot, e')$ eine Untergruppe, so auch $U = f^{-1}(V) \leq (G, *, e)$. Somit ist der Kern $\ker(f) := f^{-1}(\{e'\}) \leq (G, *)$ eine Untergruppe.

(4) Genau dann ist f injektiv, wenn $\ker(f) = \{e\}$ gilt. Allgemein:

(5) Für $a \in G$ gilt $b = f(a) \in \text{im}(f)$ und $f^{-1}(\{b\}) = a \ker(f) = \ker(f) a$.

😊 Das unscheinbare Injektivitätskriterium (4) ist überaus praktisch und wird sich im Folgenden immer wieder als hilfreich erweisen.

Arbeitssparnis: Für die Injektivität eines Gruppenhomomorphismus $f: (G, *, e) \rightarrow (H, \cdot, e')$ müssen wir nicht alle Fasern $f^{-1}(\{b\})$ prüfen, sondern nur eine einzige Faser, nämlich $\ker(f) = f^{-1}(\{e'\})$.

Homomorphismen und Untergruppen

Aufgabe: Rechnen Sie die Aussagen des Satzes sorgsam nach.

Lösung: (1) Es gilt $e' = f(e) \in V$. Zu $x, y \in V$ existieren $a, b \in U$ mit $f(a) = x$ und $f(b) = y$, also gilt $x \cdot y^{-1} = f(a) \cdot f(b)^{-1} = f(a * b^{-1}) \in V$.

(2) Die Aussage $\text{im}(f) = H$ ist die Definition von Surjektivität.

(3) Wegen $f(e) = e' \in V$ gilt $e \in U$. Seien $a, b \in U$, also $f(a), f(b) \in V$. Dann gilt $a * b^{-1} \in U$, denn $f(a * b^{-1}) = f(a) \cdot f(b)^{-1} \in V$.

(4) Die Implikation „ \Rightarrow “ ist klar. Die Umkehrung „ \Leftarrow “ folgt aus (5):

(5) Gegeben seien $a, a' \in G$ mit $f(a) = f(a')$.

- Es gilt $e' = f(a)^{-1}f(a') = f(a^{-1}a')$,
also $a^{-1}a' \in \ker(f)$, somit $a' \in a \ker(f)$.
- Es gilt $e' = f(a')f(a)^{-1} = f(a'a^{-1})$,
also $a'a^{-1} \in \ker(f)$, somit $a' \in \ker(f) a$.

◻

😊 Jede Faser ist entweder leer oder eine Translation des Kerns.

Der Satz von Cayley

Beispiel: Die Gruppe $G = (\mathbb{Z}_3, +, 0)$ bettet in $(S_G, \circ, \text{id}_G)$ ein vermöge

$$0 \mapsto \tau_0 = \begin{bmatrix} 0 & 1 & 2 \\ 0 & 1 & 2 \end{bmatrix} = \text{id},$$

$$1 \mapsto \tau_1 = \begin{bmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \end{bmatrix} = (0, 1, 2),$$

$$2 \mapsto \tau_2 = \begin{bmatrix} 0 & 1 & 2 \\ 2 & 0 & 1 \end{bmatrix} = (0, 2, 1).$$

😊 Jede noch so abstrakte Gruppe lässt sich konkret darstellen:

Satz G1s: Darstellungssatz von Cayley

Jede Gruppe $(G, *, e)$ bettet in die symmetrische Gruppe (S_G, \circ, id) ein, ist also isomorph zu einer Untergruppe $U \leq S_G$ von Permutationen.

Ist die Gruppe G endlich, von der Ordnung $n = \#G$, so gilt sogar:

Die Gruppe G bettet in die Gruppe S_n ein, ist also isomorph zu einer Untergruppe $U \leq S_n$ von Permutationen auf der Menge $\{1, \dots, n\}$.

Der Satz von Cayley

Beweis: Jedes Element $a \in G$ definiert seine Linkstranslation

$$\tau_a : G \rightarrow G : x \mapsto a * x.$$

Für $e \in G$ gilt $\tau_e = \text{id}_G$. Dank Assoziativität haben wir $\tau_{a*b} = \tau_a \circ \tau_b$:

$$(\tau_a \circ \tau_b)(x) = \tau_a(\tau_b(x)) = a * (b * x) = (a * b) * x = \tau_{a*b}(x)$$

Wir erhalten somit den gewünschten Monoidhomomorphismus

$$\tau : (G, *, e) \rightarrow (\mathbb{E}_G, \circ, \text{id}_G) : a \mapsto \tau_a.$$

Dieser ist injektiv: Für $a \neq b$ gilt $\tau_a \neq \tau_b$, denn $\tau_a(e) = a \neq b = \tau_b(e)$.

Aus $a * b = e = b * a$ folgt $\tau_a \circ \tau_b = \tau_{a*b} = \tau_e = \text{id}_G$ und $\tau_b \circ \tau_a = \text{id}_G$.

Für jedes Element $a \in G$ gilt demnach $\tau_{a^{-1}} = \tau_a^{-1}$. Wir erhalten so

$$\tau : (G, *, e) \hookrightarrow (\mathbb{S}_G, \circ, \text{id}_G) : a \mapsto \tau_a.$$

Für die Untergruppe $U = \tau(G) \leq \mathbb{S}_G$ gilt somit $\tau : G \xrightarrow{\sim} U$.

□ QED

Der Satz von Cayley

Ist die Gruppe G endlich, von der Ordnung $n = \#G$, so gilt sogar:

Die Gruppe G bettet in die Gruppe S_n ein, ist also isomorph zu einer Untergruppe $U \leq S_n$ von Permutationen auf der Menge $\{1, \dots, n\}$.

Hierzu nummerieren wir die Elemente von G durch $\nu: \{1, \dots, n\} \xrightarrow{\sim} G$ und erhalten so einen Gruppenisomorphismus $S_G \cong S_n$. Genauer:

Aufgabe: Jede Bijektion $\nu: X \xrightarrow{\sim} Y$ definiert einen Isomorphismus von Monoiden $(\varphi, \psi): E_X \cong E_Y$ und von Gruppen $(\varphi, \psi): S_X \cong S_Y$ vermöge $\varphi(\tau) = \nu \circ \tau \circ \nu^{-1}$ und $\psi(\sigma) = \nu^{-1} \circ \sigma \circ \nu$.

Lösung: Für $\tau: X \rightarrow X$ gilt $\varphi(\tau) = \nu \circ \tau \circ \nu^{-1}: Y \rightarrow Y$, also ist φ wohldefiniert. Für $\tau = \text{id}_X$ gilt $\varphi(\text{id}_X) = \text{id}_Y$. Für $\tau, \tau': X \rightarrow X$ gilt

$$\begin{aligned} \varphi(\tau \circ \tau') &= \nu \circ (\tau \circ \tau') \circ \nu^{-1} \\ &= (\nu \circ \tau \circ \nu^{-1}) \circ (\nu \circ \tau' \circ \nu^{-1}) = \varphi(\tau) \circ \varphi(\tau'). \end{aligned}$$

Somit ist $\varphi: (E_X, \circ, \text{id}_X) \rightarrow (E_Y, \circ, \text{id}_Y)$ ein Monoidhomomorphismus.

Umgekehrt gilt dasselbe für ψ . Schließlich finden wir $\psi \circ \varphi = \text{id}$ und $\varphi \circ \psi = \text{id}$, also $(\varphi, \psi): E_X \cong E_Y$. Daraus folgt $(\varphi, \psi): S_X \cong S_Y$.

Der Satz von Cayley

Der Satz von Cayley gilt wörtlich ebenso für Monoide:

Jedes Monoid $(G, *, e)$ bettet in das Abbildungsmonoid (E_G, \circ, id) ein, ist also isomorph zu einem Untermonoid $U \leq E_G$ von Abbildungen.

Ist das Monoid G endlich, von der Ordnung $n = \#G$, so gilt sogar: Das Monoid $(G, *, e)$ bettet in das Abbildungsmonoid (E_n, \circ, id) ein.

😊 Solche Abbildungen und Permutationen sind wunderbar konkrete Objekte, mit denen wir bequem, explizit und effizient rechnen können. Die Grundlagen hierzu kennen Sie von Beginn des Kapitels E.

Übung: Wenn wir Rechtstranslationen $\tau_a : x \mapsto x * a$ betrachten, so erhalten wir eine Einbettung $\tau : (G, *, e) \hookrightarrow (E_G, \bullet, \text{id}_G)$.

Übung: Die entgegengesetzten Gruppen $(S_X, \circ, \text{id}_X)$ und $(S_X, \bullet, \text{id}_X)$ sind isomorph vermöge der Inversion $\varphi : S_X \rightarrow S_X : \sigma \mapsto \sigma^{-1}$.

Übung: Die entgegengesetzten Monoide $(E_X, \circ, \text{id}_X)$ und $(E_X, \bullet, \text{id}_X)$ sind nicht isomorph für $\#X \geq 2$: Sei $c : X \rightarrow X$ eine konstante Abbildung. In $(E_X, \circ, \text{id}_X)$ gilt dann $c \circ f = c$ für alle $f \in E_X$. Hingegen gibt es in $(E_X, \bullet, \text{id}_X)$ kein Element c' mit $c' \bullet f = c'$ für alle $f \in E_X$.

Summen und Produkte

Sei $(M, +, 0)$ bzw. $(M, \cdot, 1)$ ein Monoid, hier additiv oder multiplikativ geschrieben. Mehrfache Summen und Produkte definieren wir rekursiv:

$$\sum_{i=1}^0 a_i := 0, \quad \sum_{i=1}^{n+1} a_i := \left(\sum_{i=1}^n a_i \right) + a_{n+1} = (\dots (a_1 + a_2) + \dots) + a_{n+1}$$

$$\prod_{i=1}^0 a_i := 1, \quad \prod_{i=1}^{n+1} a_i := \left(\prod_{i=1}^n a_i \right) \cdot a_{n+1} = (\dots (a_1 \cdot a_2) \cdot \dots) \cdot a_{n+1}$$

Dank Assoziativität können wir beliebig umklammern,
bei kommutierenden Elementen auch beliebig umordnen:

Ist $I = \{i_1, i_2, \dots, i_n\}$ eine n -elementige Menge, so schreiben wir

$$\sum_{i \in I} a_i := \sum_{k=1}^n a_{i_k} \quad \text{und} \quad \prod_{i \in I} a_i := \prod_{k=1}^n a_{i_k}.$$

Eine Umnummerierung der Elemente ändert das Ergebnis nicht.

Sei J eine Menge und $I \subseteq J$ endlich, sodass $a_i = 0$ für alle $i \in J \setminus I$.
Dann definieren wir $\sum_{i \in J} a_i := \sum_{i \in I} a_i$ als endliche Summe wie oben.

Vielfache und Potenzen

Für $n \in \mathbb{N}$ definieren wir das n te Vielfache und die n te Potenz durch

$$a \cdot n := \sum_{i=1}^n a \quad \text{und} \quad a^n := \prod_{i=1}^n a.$$

Ist $-a$ das Negative zu a in $(M, +, 0)$, so setzen wir $a \cdot (-n) := (-a) \cdot n$.

Ist a^{-1} das Inverse zu a in $(M, \cdot, 1)$, so setzen wir $a^{-n} := (a^{-1})^n$.

Auf dem Monoid M bzw. der Gruppe M^\times definiert dies die Operationen

$$M \times \mathbb{N} \rightarrow M : (a, n) \mapsto a \cdot n, \quad M^\times \times \mathbb{Z} \rightarrow M^\times : (a, n) \mapsto a \cdot n,$$

$$M \times \mathbb{N} \rightarrow M : (a, n) \mapsto a^n, \quad M^\times \times \mathbb{Z} \rightarrow M^\times : (a, n) \mapsto a^n.$$

Wir schreiben $a \cdot n = n \cdot a$ von rechts oder von links, kurz $an = na$.

Satz G1T: Rechenregeln für Vielfache und Potenzen

Für alle $a \in M$ und $m, n \in \mathbb{N}$ bzw. $a \in M^\times$ und $m, n \in \mathbb{Z}$ gilt:

$$a \cdot 0 = 0, \quad a \cdot 1 = a, \quad a \cdot (m + n) = a \cdot m + a \cdot n, \quad a \cdot (m \cdot n) = (a \cdot m) \cdot n,$$

$$a^0 = 1, \quad a^1 = a, \quad a^{m+n} = a^m \cdot a^n, \quad a^{m \cdot n} = (a^m)^n.$$

Kommutieren: Aus $a + b = b + a$ folgt $(a + b) \cdot n = a \cdot n + b \cdot n$.

Aus $a \cdot b = b \cdot a$ folgt entsprechend $(a \cdot b)^n = a^n \cdot b^n$.

Das erzeugte Untermonoid und die erzeugte Untergruppe

Satz G1U: erzeugtes Untermonoid und erzeugte Untergruppe

Sei $(M, \cdot, 1)$ ein Monoid und $S \subseteq M$ eine Teilmenge.

(1) Das von $S \subseteq M$ in $(M, \cdot, 1)$ **erzeugte Untermonoid** ist

$$[S] := \{ s_1^{e_1} s_2^{e_2} \cdots s_n^{e_n} \mid n \in \mathbb{N}, s_i \in S, e_i \in \mathbb{N} \}.$$

Dies ist ein Untermonoid in M und zudem das kleinste, das S enthält.

(2) Die von $S \subseteq M^\times$ in $(M, \cdot, 1)$ **erzeugte Untergruppe** ist

$$\langle S \rangle := \{ s_1^{e_1} s_2^{e_2} \cdots s_n^{e_n} \mid n \in \mathbb{N}, s_i \in S, e_i \in \mathbb{Z} \}.$$

Dies ist eine Untergruppe in M und zudem die kleinste, die S enthält.

Die Inversion auf S ist dabei gegeben durch

$$(s_1^{e_1} s_2^{e_2} \cdots s_n^{e_n})^{-1} = s_n^{-e_n} \cdots s_2^{-e_2} s_1^{-e_1}.$$

Übung: Beweisen Sie die Behauptungen des Satzes. Was ist zu tun?

Beispiel: In der Gruppe (S_4, \circ, id) gilt $\langle (1, 2), (2, 3) \rangle = S_3$.

Beispiele zu Homomorphismen und Untergruppen

Sei $(M, \cdot, 1)$ ein Monoid, hier multiplikativ geschrieben.

(1) Zu jedem Element $a \in M$ haben wir den Monoidhomomorphismus

$$\psi : (\mathbb{N}, +, 0) \rightarrow (M, \cdot, 1) : n \mapsto a^n.$$

Sein Bild ist das von a in $(M, \cdot, 1)$ erzeugte Untermonoid:

$$\text{im}(\psi) = \{ a^n \mid n \in \mathbb{N} \} =: [a]$$

(2) Zu jedem $a \in M^\times$ haben wir den Gruppenhomomorphismus

$$\varphi : (\mathbb{Z}, +, 0) \rightarrow (M, \cdot, 1) : n \mapsto a^n.$$

Sein Bild ist die von a in $(M, \cdot, 1)$ erzeugte Untergruppe:

$$\text{im}(\varphi) = \{ a^n \mid n \in \mathbb{Z} \} =: \langle a \rangle$$

In additiver Schreibweise $(M, +, 0)$ gilt entsprechend

$$[a] = a\mathbb{N} = a \cdot \mathbb{N} = \{ a \cdot n \mid n \in \mathbb{N} \},$$

$$\langle a \rangle = a\mathbb{Z} = a \cdot \mathbb{Z} = \{ a \cdot n \mid n \in \mathbb{Z} \}.$$

Wir nennen $\text{ord}(a) := \# \langle a \rangle$ die Ordnung von a in der Gruppe M^\times .

Klassifikation der Untergruppen von $(\mathbb{Z}, +)$

Beispiel: Für $n \in \mathbb{N}$ ist die Menge $n\mathbb{Z}$ eine Untergruppe von $(\mathbb{Z}, +)$. Dabei ist $0\mathbb{Z} = \{0\}$ die triviale Gruppe und $1\mathbb{Z} = \mathbb{Z}$ die gesamte Gruppe.

Satz G1v: Klassifikation der Untergruppen von $(\mathbb{Z}, +)$

Zu jeder Untergruppe $H \leq (\mathbb{Z}, +)$ existiert $n \in \mathbb{N}$, sodass $H = n\mathbb{Z}$ gilt.

Beweis: Ist $H = \{0\}$, so haben wir $H = 0\mathbb{Z}$.

Andernfalls existiert ein Element $a \in H$ mit $a \neq 0$.

Wir können $a > 0$ annehmen, denn auch $-a$ liegt in H .

Somit existiert $n = \min\{a \in H \mid a > 0\}$ dank Satz F1s.

Aus $n \in H \leq (\mathbb{Z}, +)$ folgt zunächst $\langle n \rangle = n\mathbb{Z} \subseteq H$.

Wir zeigen nun die Umkehrung $H \subseteq n\mathbb{Z}$. Hierzu sei $a \in H$.

Euklidische Division ergibt $a = nq + r$ mit $q, r \in \mathbb{Z}$ und $0 \leq r < n$.

Wegen $r = a - nq \in H$ folgt $r = 0$, denn n ist minimal.

Also gilt $a = nq \in n\mathbb{Z}$. Dies zeigt $H \subseteq n\mathbb{Z}$.

Damit ist $H = n\mathbb{Z}$ bewiesen.

QED

Zyklische Untermonoide

Sei $(M, \cdot, 1)$ ein Monoid und $a \in M$ ein Element. Wie sieht das erzeugte Monoid $[a]$ aus? Hierzu betrachten wir den Monoidhomomorphismus

$$\psi : (\mathbb{N}, +, 0) \rightarrow (M, \cdot, 1) : k \mapsto a^k.$$

Sein Bild ist $[a] = \{ a^k \mid k \in \mathbb{N} \}$. Ist ψ injektiv, so haben wir

$$\hat{\psi} : (\mathbb{N}, +, 0) \xrightarrow{\sim} ([a], \cdot, 1) : k \mapsto a^k.$$

Andernfalls existieren $0 \leq m < n$ in \mathbb{N} , sodass ψ auf $\{0, \dots, n-1\}$ injektiv ist und dann $a^n = a^m$ gilt. Graphisch bedeutet das folgendes:

$$a^0 \mapsto a^1 \mapsto a^2 \mapsto \dots \mapsto a^m \mapsto a^{m+1} \mapsto \dots \mapsto a^{n-1} \mapsto a^n$$

Demnach ist $n = \sharp[a]$ die Ordnung des erzeugten Untermonoids. Im Falle $0 < m < n$ gilt zudem $a^{m-1} \neq a^{n-1}$, aber $a^{m-1} \cdot a = a^{n-1} \cdot a$. Somit ist a nicht kürzbar, also insbesondere auch nicht invertierbar.

😊 Ist a in $(M, \cdot, 1)$ invertierbar und $n = \sharp[a] < \infty$, so gilt $m = 0$. Somit ist $[a] = \langle a \rangle$ eine „zyklische Gruppe“. Der folgende Satz führt dies aus.

Zyklische Untergruppen

Beispiel: In der Gruppe (S_5, \circ, id) betrachten wir $\sigma = (1, 2)(3, 4, 5)$:

$$\begin{aligned} \sigma^0 &= \text{id}, & \sigma^1 &= (1, 2)(3, 4, 5), & \sigma^2 &= (3, 5, 4), \\ \sigma^3 &= (1, 2), & \sigma^4 &= (3, 4, 5), & \sigma^5 &= (1, 2)(3, 5, 4), \\ \sigma^6 &= \text{id}, & \sigma^7 &= \sigma, & \dots & \sigma^k = (1, 2)^k(3, 4, 5)^k. \end{aligned}$$

In (S_5, \circ, id) erhalten wir so eine Untergruppe $\langle \sigma \rangle \cong \mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}_6$.

Satz G1w: zyklische Untergruppe und Ordnung eines Elements

Sei $(G, *)$ eine Gruppe und $a \in G$ ein Element. Dazu betrachten wir den Gruppenhomomorphismus $\varphi: (\mathbb{Z}, +) \rightarrow (G, *): k \mapsto a^k$.

Sein Bild ist die Untergruppe $\langle a \rangle = \{ a^k \mid k \in \mathbb{Z} \}$ in $(G, *)$.

Der Kern erfüllt $\ker(\varphi) = n\mathbb{Z}$ für ein $n \in \mathbb{N}$ dank Satz G1v.

- 0** Im Falle $n = 0$ hat a unendliche Ordnung, $\text{ord}(a) = \#\langle a \rangle = \infty$,
und wir erhalten den Gruppenisomorphismus $\hat{\varphi}: \mathbb{Z} \xrightarrow{\sim} \langle a \rangle: k \mapsto a^k$.
- 1** Im Falle $n \geq 1$ hat a endliche Ordnung, $\text{ord}(a) = \#\langle a \rangle = n$,
und wir erhalten den Isomorphismus $\bar{\varphi}: \mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} \langle a \rangle: [k] \mapsto a^k$.

Zyklische Untergruppen

Beweis: (1) Allein die Konstruktion von $\bar{\varphi}$ bedarf der Erläuterung.

Wir haben $\varphi: \mathbb{Z} \rightarrow G: k \mapsto a^k$ mit $\ker(\varphi) = n\mathbb{Z}$. Für alle $k, \ell \in \mathbb{Z}$ gilt demnach $\varphi(k) = \varphi(\ell)$ genau dann, wenn $k - \ell \in n\mathbb{Z}$ (G1R).

Aus φ erhalten wir $\bar{\varphi}$ durch die kanonische Faktorisierung E3:

$$\begin{array}{ccc}
 (\mathbb{Z}, +) & \xrightarrow{\varphi: k \mapsto a^k} & (G, *) \\
 \downarrow q & \searrow \hat{\varphi} & \uparrow \iota \\
 \mathbb{Z}/n\mathbb{Z} & \xrightarrow{\bar{\varphi}: [k] \mapsto a^k} & \langle a \rangle
 \end{array}$$

$q: [x] \mapsto [y]$ (down arrow)
 $\iota: a^k \mapsto a^k$ (up arrow)

Dank dieser Konstruktion ist $\bar{\varphi}$ bijektiv. Zudem ist $\bar{\varphi}$ ein Homomorphismus, denn $[k] + [\ell] = [k + \ell] \mapsto a^{k+\ell} = a^k \cdot a^\ell$.

(0) Im Falle $n = 0$ ist $q: (\mathbb{Z}, +) \rightarrow (\mathbb{Z}/0\mathbb{Z}, +)$ ein Isomorphismus.

In diesem Falle ist $\hat{\varphi}: (\mathbb{Z}, +) \xrightarrow{\sim} (\langle a \rangle, \cdot)$ ein Isomorphismus. ◻

Übung: Ist $\sigma = \sigma_1 \circ \dots \circ \sigma_m$ in (S_N, \circ, id) ein Produkt disjunkter Zyklen der Länge ℓ_1, \dots, ℓ_m , dann hat σ die Ordnung $\text{ord}(\sigma) = \text{kgV}(\ell_1, \dots, \ell_m)$.

Kartesisches Produkt mit koordinatenweiser Verknüpfung

Beispiel: Mit koordinatenweiser Verknüpfung ist $(\mathbb{R}^n, +, 0, -)$ eine abelsche Gruppe. Gleiches gilt für $\mathbb{R}^{\mathbb{N}}$ und $\mathbb{R}^{(\mathbb{N})}$. Ausführlich:

Beispiel G1x: Produkt $G_1 \times \dots \times G_n$ von Gruppen

Ist $(G_i, *_i, e_i, {}^{-1})$ eine Gruppe für $i = 1, \dots, n$, so auch das Produkt

$$(G, *, e, {}^{-1}) \quad \text{mit} \quad G = G_1 \times \dots \times G_n,$$

$$(a_1, \dots, a_n) * (b_1, \dots, b_n) = (a_1 *_1 b_1, \dots, a_n *_n b_n),$$

$$e = (e_1, \dots, e_n) \quad \text{und} \quad (a_1, \dots, a_n)^{-1} = (a_1^{-1}, \dots, a_n^{-1}).$$

Die Projektion $\text{pr}_i: G \rightarrow G_i: a \mapsto a_i$ ist ein Gruppenhomomorphismus, ebenso die Einbettung $\iota_i: G_i \hookrightarrow G: a_i \mapsto (e_1, \dots, a_i, \dots, e_n)$.

Gleiches gilt sinngemäß für das Produkt von Monoiden $(G_i, *_i, e_i)$. Genau dann ist G kommutativ, wenn alle G_1, \dots, G_n dies sind.

Übung: Rechnen Sie dieses und das nächste Beispiel sorgsam nach. Diese Konstruktionen sind grundlegend und werden uns oft nützen.

Funktionen mit punktweiser Verknüpfung

Beispiel G1Y: Potenz G^Ω und $G^{(\Omega)}$ einer Gruppe

(1) Sei Ω eine Menge. Ist $(G, +, 0, -)$ eine Gruppe, so auch die Potenz

$$(G, +, 0, -)^\Omega = (G^\Omega, \mathbf{+}, \mathbf{0}, \mathbf{-}) \text{ mit } G^\Omega = \text{Abb}(\Omega, G) = \{ f : \Omega \rightarrow G \},$$

$$(f \mathbf{+} g)(x) = f(x) + g(x), \quad \mathbf{0} : \Omega \rightarrow G : x \mapsto 0 \text{ und } (\mathbf{-}f)(x) = -f(x).$$

Hierbei ist $\text{pr}_x : G^\Omega \rightarrow G : f \mapsto f(x)$ ein Gruppenhomomorphismus, ebenso $\iota_x : G \hookrightarrow G^\Omega : a \mapsto f$ mit $f(x) = a$ und $f(y) = 0$ für $y \neq x$.

(2) Für den Träger $\text{supp}(f) = \{ x \in \Omega \mid f(x) \neq 0 \}$ gilt $\text{supp}(\mathbf{0}) = \emptyset$ und $\text{supp}(\mathbf{-}f) = \text{supp}(f)$ sowie $\text{supp}(f \mathbf{+} g) \subseteq \text{supp}(f) \cup \text{supp}(g)$. In G^Ω liegt somit die Untergruppe der Funktionen mit endlichem Träger:

$$G^{(\Omega)} = \{ f : \Omega \rightarrow G \mid \#\text{supp}(f) < \infty \}$$

Gleiches gilt sinngemäß für die Potenz eines Monoids $(G, +, 0)$. Genau dann sind G^Ω und $G^{(\Omega)}$ kommutativ, wenn G dies ist.

Beispiel G1Z: Fundamentalsatz der Arithmetik

Sei $\mathbb{P} = \{2, 3, 5, 7, \dots\}$ die Menge der Primzahlen in $(\mathbb{N}_{\geq 1}, \cdot)$.

Wir betrachten die Menge $\mathbb{N}^{(\mathbb{P})} = \{e : \mathbb{P} \rightarrow \mathbb{N} \mid \#\text{supp}(e) < \infty\}$.

(1) Hierzu haben wir den Monoidhomomorphismus

$$\Phi : (\mathbb{N}^{(\mathbb{P})}, +) \xrightarrow{\sim} (\mathbb{N}_{\geq 1}, \cdot) : e \mapsto \prod_{p \in \mathbb{P}} p^{e(p)}.$$

Ausgeschrieben ist dies das (endliche!) Produkt $2^{e(2)} \cdot 3^{e(3)} \cdot 5^{e(5)} \dots$.

Dank Fundamentalsatz der Arithmetik A2J ist Φ ein Isomorphismus.

(2) Übergang zu Brüchen ergibt den Gruppenisomorphismus

$$\Phi : (\mathbb{Z}^{(\mathbb{P})}, +) \xrightarrow{\sim} (\mathbb{Q}_{>0}, \cdot) : e \mapsto \prod_{p \in \mathbb{P}} p^{e(p)}.$$

(3) Hinzufügen des Vorzeichens \pm ergibt die Isomorphismen

$$\Phi : (\mathbb{Z}/2, +) \times (\mathbb{N}^{(\mathbb{P})}, +) \xrightarrow{\sim} (\mathbb{Z}^*, \cdot) : (s, e) \mapsto (-1)^s \prod_{p \in \mathbb{P}} p^{e(p)},$$

$$\Phi : (\mathbb{Z}/2, +) \times (\mathbb{Z}^{(\mathbb{P})}, +) \xrightarrow{\sim} (\mathbb{Q}^*, \cdot) : (s, e) \mapsto (-1)^s \prod_{p \in \mathbb{P}} p^{e(p)}.$$

Fundamentalsatz der Arithmetik als Isomorphismus

😊 Abstrakte Theorie wirkt ganz konkret! Die Umkehrfunktion $\Phi^{-1} : (\mathbb{N}^*, \cdot) \rightarrow (\mathbb{N}^{(\mathbb{P})}, +)$ ist die Primfaktorzerlegung und notorisch schwer zu berechnen. Genau darauf beruhen Cryptosysteme wie RSA.

Aufgabe: Ist $\sqrt[3]{72/125}$ rational? Nutzen Sie den Isomorphismus Φ !

Lösung: Als Primfaktorzerlegung finden wir hier $72/125 = 2^3 3^2 5^{-3}$. In $\mathbb{Z}^{(\mathbb{P})}$ können wir $\Phi^{-1}(72/125) = (3, 2, -3, 0, \dots)$ nicht durch 3 teilen. In $(\mathbb{Q}_{>0}, \cdot)$ können wir aus $72/125$ demnach nicht die 3te Wurzel ziehen.

Aufgabe: Wir kennen den Isomorphismus $(\exp, \ln) : (\mathbb{R}, +) \cong (\mathbb{R}_{>0}, \cdot)$. Existiert ebenso ein Isomorphismus $(\varphi, \psi) : (\mathbb{Q}, +) \cong (\mathbb{Q}_{>0}, \cdot)$?

Lösung: Nein! In $(\mathbb{Q}, +)$ können wir jedes Element durch 2 dividieren, aber in $(\mathbb{Q}_{>0}, \cdot)$ nicht aus jedem Element die Quadratwurzel ziehen, zum Beispiel ist $\sqrt{2}$ irrational, siehe Satz A1F.

Übung: Existiert ein Isomorphismus $(\varphi, \psi) : (\mathbb{C}, +) \cong (\mathbb{C}^\times, \cdot)$?

Betrag und Vorzeichen reeller Zahlen

Beispiel: Für reelle Zahlen haben wir den **Absolutbetrag**

$$|-| : \mathbb{R} \rightarrow \mathbb{R}_{\geq 0} : x \mapsto |x| = \begin{cases} +x & \text{falls } x \geq 0, \\ -x & \text{falls } x \leq 0, \end{cases}$$

und das **Vorzeichen**

$$\text{sign} : \mathbb{R} \rightarrow \{\pm 1, 0\} : x \mapsto \begin{cases} +1 & \text{falls } x > 0, \\ -1 & \text{falls } x < 0, \\ 0 & \text{falls } x = 0. \end{cases}$$

Beide sind multiplikativ, genauer Monoidhomomorphismen, denn es gilt $|1| = 1$ und $|x \cdot y| = |x| \cdot |y|$ für alle $x, y \in \mathbb{R}$, sowie $\text{sign}(1) = 1$ und $\text{sign}(x \cdot y) = \text{sign}(x) \cdot \text{sign}(y)$.

Für jedes invertierbare Element $x \in \mathbb{R}^\times = \mathbb{R} \setminus \{0\}$ sind auch $|x|$ und $\text{sign}(x)$ invertierbar, und es gilt $|x^{-1}| = |x|^{-1}$ und $\text{sign}(x^{-1}) = \text{sign}(x)^{-1} = \text{sign}(x)$.

Betrag und Vorzeichen reeller Zahlen

Durch Einschränkung erhalten wir die Gruppenhomomorphismen

$$\begin{aligned} |-\!| &: (\mathbb{R}^\times, \cdot, 1) \twoheadrightarrow (\mathbb{R}_{>0}, \cdot, 1), \\ \text{sign} &: (\mathbb{R}^\times, \cdot, 1) \twoheadrightarrow (\{\pm 1\}, \cdot, 1). \end{aligned}$$

Zusammengesetzt erhalten wir den Gruppenisomorphismus:

$$(\varphi, \psi) : \mathbb{R}^\times \cong \{\pm 1\} \times \mathbb{R}_{>0}$$

Hierbei ist $\varphi(x) = (\text{sign}(x), |x|)$ und $\psi(s, r) = s \cdot r$.

Beide Abbildungen sind Gruppenhomomorphismen, und nach Konstruktion gilt $\psi \circ \varphi = \text{id}$ und $\varphi \circ \psi = \text{id}$.

Der Absolutbetrag $|x|$ heißt auch **Norm** und misst den Abstand von x zum Nullpunkt. Insbesondere erhalten wir so die Menge

$$\mathbb{S}^0 := \{ x \in \mathbb{R} \mid |x| = 1 \} = \{-1, +1\}.$$

Dies ist der Kern von $x \mapsto |x|$. Ebenso gilt $\mathbb{R}_{>0} = \ker(\text{sign})$.

Betrag und Richtung komplexer Zahlen

Beispiel: Auch für komplexe Zahlen haben wir den **Absolutbetrag**

$$|\cdot| : \mathbb{C} \rightarrow \mathbb{R}_{\geq 0} : z = x + iy \mapsto |z| = \sqrt{x^2 + y^2}.$$

Dies heißt auch **Norm** und misst den Abstand von z zum Nullpunkt. Somit ist die Menge $\mathbb{S}^1 := \{z \in \mathbb{C} \mid |z| = 1\}$ die Einheitskreislinie.

Analog zum Vorzeichen reeller Zahlen definieren wir die **Richtung**

$$\text{sign} : \mathbb{C} \rightarrow \mathbb{S}^1 \sqcup \{0\} : z \mapsto \begin{cases} z/|z| & \text{falls } z \neq 0, \\ 0 & \text{falls } z = 0. \end{cases}$$

Beide sind multiplikativ, genauer Monoidhomomorphismen, denn es gilt $|1| = 1$ und $|z \cdot w| = |z| \cdot |w|$ für alle $z, w \in \mathbb{C}$, und somit $\text{sign}(1) = 1$ und $\text{sign}(z \cdot w) = \text{sign}(z) \cdot \text{sign}(w)$.

Für jedes invertierbare Element $z \in \mathbb{C}^\times = \mathbb{C} \setminus \{0\}$ sind auch $|z|$ und $\text{sign}(z)$ invertierbar, und es gilt $|z^{-1}| = |z|^{-1}$ und $\text{sign}(z^{-1}) = \text{sign}(z)^{-1} = \overline{\text{sign}(z)}$.

Betrag und Richtung komplexer Zahlen

Durch Einschränkung erhalten wir die Gruppenhomomorphismen

$$\begin{aligned} |\cdot| &: (\mathbb{C}^\times, \cdot, 1) \twoheadrightarrow (\mathbb{R}_{>0}, \cdot, 1), \\ \text{sign} &: (\mathbb{C}^\times, \cdot, 1) \twoheadrightarrow (\mathbb{S}^1, \cdot, 1). \end{aligned}$$

Diese sind surjektiv mit $\ker(z \mapsto |z|) = \mathbb{S}^1$ und $\ker(\text{sign}) = \mathbb{R}_{>0}$.

Zusammengesetzt erhalten wir den Gruppenisomorphismus:

$$(\varphi, \psi) : \mathbb{C}^\times \cong \mathbb{S}^1 \times \mathbb{R}_{>0}$$

Hierbei ist $\varphi(z) = (\text{sign}(z), |z|)$ und $\psi(s, r) = s \cdot r$.

Beide Abbildungen sind Gruppenhomomorphismen, und nach Konstruktion gilt $\psi \circ \varphi = \text{id}$ und $\varphi \circ \psi = \text{id}$.

Eingeschränkt auf \mathbb{R} gilt $\mathbb{C}^\times \cap \mathbb{R} = \mathbb{R}^\times$ und $\mathbb{S}^1 \cap \mathbb{R} = \mathbb{S}^0$, und wir erhalten erneut den obigen Gruppenisomorphismus

$$\mathbb{R}^\times \cong \mathbb{S}^0 \times \mathbb{R}_{>0}.$$

Definition G2A: Ring und Körper

Ein [kommutativer] **Ring** $(R, +, 0, \cdot, 1)$ besteht aus einer Menge R mit Verknüpfungen $+, \cdot : R \times R \rightarrow R$ und Elementen $0, 1 \in R$, sodass gilt:

- 0 Für alle Elemente $a, b, c \in R$ gelten die Distributivgesetze $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ und $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$.
- 1 $(R, +, 0)$ ist eine kommutative Gruppe.
- 2 $(R, \cdot, 1)$ ist ein [kommutatives] Monoid.

Wir setzen $R^* := R \setminus \{0\}$. Der Ring $(R, +, 0, \cdot, 1)$ heißt

- **Divisionsring**, wenn $R^* < (R, \cdot, 1)$ eine Gruppe ist.
- **Körper**, wenn $R^* < (R, \cdot, 1)$ eine kommutative Gruppe ist.
- **Integritätsring**, wenn $R^* < (R, \cdot, 1)$ ein kommutatives Monoid ist.

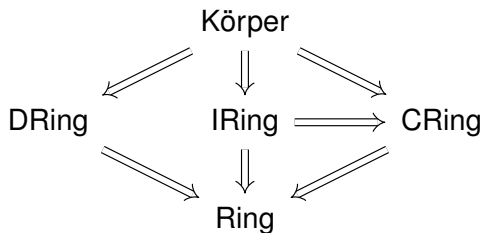
Für den Ring $(R, +, 0, \cdot, 1)$ schreiben wir auch $(R, +, \cdot)$ oder kurz R .

Beispiele: Wir haben die Ringe $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C} \subset \mathbb{H}$ sowie $\mathbb{Z}/n\mathbb{Z}$.

Der Nullring $(\{0\}, +, 0, \cdot, 1)$ ist ein Ring, und zwar der einzige mit $1 = 0$.

Ringe und Körper: Definition

Überblick:



$(R, +, 0, \cdot, 1)$		$(R, +, 0)$				$(R, +, \cdot)$		$(R, \cdot, 1)$					
Name	Beispiele	Ass	Ntr	Inv	Com	DL	DR	Ass	Ntr	$1 \neq 0$	Ntf	Inv^*	Com
Körper	$\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p$	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
DRing	$\mathbb{H} \subset \mathbb{C}^{2 \times 2}$	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
IRing	$\mathbb{Z}, \mathbb{Q}[X]$	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓
CRing	$\mathbb{Z}_n, \mathbb{R}^\Omega$	✓	✓	✓	✓	✓	✓	✓	✓				✓
Ring	$\mathbb{R}^{2 \times 2}$	✓	✓	✓	✓	✓	✓	✓	✓				

Statt explizit $(R, +, 0, \cdot, 1)$ schreiben wir auch kurz implizit $(R, +, \cdot)$; die neutralen Elemente 0 und 1 sind daraus eindeutig rekonstruierbar.

Ringe und Körper: Definition

Hier steht „Ntf“ für Nullteilerfreiheit, also $a \neq 0 \wedge b \neq 0 \Rightarrow a \cdot b \neq 0$
bzw. äquivalent hierzu $a \cdot b = 0 \Rightarrow a = 0 \vee b = 0$ für alle $a, b \in R$.

Ich nutze die bequemen Abkürzungen

- „DRing“ für Divisionsring (engl. *division ring*, *division algebra*),
- „IRing“ für Integritätsring (engl. *integral ring*, *integral domain*),
- „CRing“ für kommutativer Ring (engl. *commutative ring*).

Auch bei kommutativen Ringen möchte ich meist $1 \neq 0$ fordern,
ich scheue mich jedoch, dies in die Definition aufzunehmen.

Wir müssen es daher bei Bedarf jeweils explizit fordern.

Muss es wirklich so allgemein sein? Dazu gibt es sehr verschiedene
Ansichten. Am liebsten wäre mir Lineare Algebra allein über Körpern.

Doch dieser Wunsch nach Einfachheit stößt sich schnell an der Realität:
Eher früher als später benötigen wir Matrixringe und Polynomringe, etc.

Ich halte es daher für besser, Sie von Anfang an auf die nötige Vielfalt
sanft vorzubereiten. Umso mehr schätzen wir die heile Welt der Körper.

Ringe und Körper: logische Spitzfindigkeit

In der Definition G2A eines Rings $(R, +, 0, \cdot, 1)$ muss die Kommutativität der Addition nicht gefordert werden, sie folgt aus den anderen Axiomen:

Aufgabe: Gegeben sei $(R, +, 0, \cdot, 1)$ mit $+, \cdot : R \times R \rightarrow R$ und $0, 1 \in R$, so dass beide Distributivgesetze gelten und zudem:

1 $(R, +, 0)$ ist eine Gruppe.

2 $(R, \cdot, 1)$ ist ein Monoid.

Dann ist $(R, +, 0)$ kommutativ und somit $(R, +, 0, \cdot, 1)$ ein Ring.

Lösung: Wir entwickeln $(1 + 1) \cdot (a + b)$ auf zwei Arten:

$$(1 + 1) \cdot (a + b) \stackrel{\text{DR}}{=} 1 \cdot (a + b) + 1 \cdot (a + b) \stackrel{\text{Ntr}}{=} a + b + a + b$$

$$(1 + 1) \cdot (a + b) \stackrel{\text{DL}}{=} (1 + 1) \cdot a + (1 + 1) \cdot b$$

$$\stackrel{\text{DR}}{=} 1 \cdot a + 1 \cdot a + 1 \cdot b + 1 \cdot b \stackrel{\text{Ntr}}{=} a + a + b + b$$

Wir addieren $-a$ von links, $-b$ von rechts und erhalten $a + b = b + a$.

Bemerkung: Hierzu genügt, dass $(R, +, 0)$ ein kürzbares Monoid ist. Dasselbe Argument gilt also auch für Halbringe mit kürzbarer Addition.

Lemma G2B

In jedem Ring $(R, +, 0, \cdot, 1)$ gilt für alle $a, b \in R$:

- 1 $0 \cdot a = 0 = a \cdot 0$.
- 2 $(-a) \cdot b = a \cdot (-b) = -(a \cdot b)$
- 3 $(-a) \cdot (-b) = a \cdot b$

Beweis: (1) Es gilt $0 \cdot a = (0 + 0) \cdot a = (0 \cdot a) + (0 \cdot a)$.

Addition von $-(0 \cdot a)$ ergibt $0 = 0 \cdot a$. Ebenso folgt $a \cdot 0 = 0$.

(2) Es gilt $(a \cdot b) + ((-a) \cdot b) = (a + (-a)) \cdot b = 0 \cdot b = 0$,
ebenso $(a \cdot b) + (a \cdot (-b)) = a \cdot (b + (-b)) = a \cdot 0 = 0$.

(3) Es folgt $(-a) \cdot (-b) = -(a \cdot (-b)) = -(-(a \cdot b)) = a \cdot b$. □

Folgerung: Ist $(R, +, 0, \cdot, 1)$ ein Ring mit $1 = 0$, so folgt $R = \{0\}$,
denn für jedes Element $a \in R$ gilt dann $a = 1 \cdot a = 0 \cdot a = 0$.

Konvention: Wir sparen Klammern und schreiben $(a \cdot b) + c = a \cdot b + c$
(Punkt vor Strich). Für die Multiplikation schreiben wir statt $a \cdot b$ kurz ab .

Lemma G2c

In jedem Körper / Divisionsring / Integritätsring $(R, +, 0, \cdot, 1)$ gilt:

- 1 Die Menge R enthält mindestens zwei Elemente:

$$1 \neq 0$$

- 2 Nullteilerfreiheit:

$$a \neq 0 \wedge b \neq 0 \Rightarrow a \cdot b \neq 0$$

$$a \cdot b = 0 \Rightarrow a = 0 \vee b = 0$$

- 3 Kürzbarkeit:

$$a \cdot x = a \cdot y \wedge a \neq 0 \Rightarrow x = y$$

$$x \cdot a = y \cdot a \wedge a \neq 0 \Rightarrow x = y$$

Beweis: (1) Das Untermonoid $R^* = R \setminus \{0\}$ enthält das Einselement 1.

(2) Abgeschlossenheit von $R^* < (R, \cdot, 1)$: Aus $a, b \in R^*$ folgt $a \cdot b \in R^*$.

(3) Aus $a \cdot x = a \cdot y$ folgt $0 = a \cdot x - a \cdot y = a \cdot (x - y)$.

Dank $a \neq 0$ und (2) folgt $x - y = 0$, somit $x = y$.

□ QED

Satz G2D: allgemeine Distributivität und binomische Formeln

(1) In jedem Ring R gilt das allgemeine Distributivitätsgesetz:

$$\left(\sum_{i \in I} a_i\right) \cdot \left(\sum_{j \in J} b_j\right) = \sum_{(i,j) \in I \times J} a_i \cdot b_j = \sum_{i \in I} \sum_{j \in J} a_i b_j = \sum_{j \in J} \sum_{i \in I} a_i b_j$$

Seien $a, b \in R$ kommutierende Elemente, also $ab = ba$. Dann gilt

$$(a + b)^2 = a^2 + 2ab + b^2 \quad \text{und} \quad (a - b)(a + b) = a^2 - b^2.$$

Allgemein für alle $n \in \mathbb{N}$ gilt hierzu (2) der binomische Lehrsatz

$$(a + b)^n = \sum_{i=0}^n \binom{n}{i} a^i b^{n-i} = \sum_{j=0}^n \binom{n}{j} a^{n-j} b^j$$

sowie (3) die geometrische Teleskopsumme

$$(a - b) \cdot \sum_{i=0}^n a^{n-i} b^i = a^{n+1} - b^{n+1}.$$

Allgemeine Distributivität und binomische Formeln

Beweis: (1) Induktion über die Elementezahl $\#I$ und $\#J$.

(2) Induktion über $n \in \mathbb{N}$ oder anschaulich wie in E2J.

(3) Induktion über $n \in \mathbb{N}$ oder anschaulich wie folgt:

$$\begin{aligned} & (a - b) \cdot (a^n b^0 + a^{n-1} b^1 + \dots + a^0 b^n) \\ &= a^{n+1} b^0 + a^n b^1 + \dots + a^1 b^n \\ &\quad - a^n b^1 - \dots - a^1 b^n - a^0 b^{n+1} \end{aligned}$$

In dieser Teleskopsumme löschen sich innere Terme paarweise aus. Schließlich bleiben nur die beiden Randterme a^{n+1} und $-b^{n+1}$ stehen.

Beispiel: Für $q \in \mathbb{C}$ mit $q \neq 1$ gilt

$$1 + q + q^2 + \dots + q^{n-1} = \frac{1 - q^n}{1 - q}.$$

Geometrische Reihe: Für $|q| < 1$ und $n \rightarrow \infty$ gilt $q^n \rightarrow 0$, und somit

$$\sum_{k=0}^{\infty} q^k = \lim_{n \rightarrow \infty} \sum_{k=0}^{n-1} q^k = \lim_{n \rightarrow \infty} \frac{1 - q^n}{1 - q} = \frac{1}{1 - q}.$$

Definition G2E: Homomorphismen von Ringen und Körpern

Seien $(R, +, 0, \cdot, 1)$ und $(S, +, 0, \cdot, 1)$ Ringe. Ein **Homomorphismus**

$$\varphi : (R, +, 0, \cdot, 1) \rightarrow (S, +, 0, \cdot, 1)$$

ist eine Abbildung $\varphi : R \rightarrow S$, sodass für alle $a, b \in R$ gilt:

$$\varphi(a + b) = \varphi(a) + \varphi(b), \quad \varphi(0) = 0,$$

$$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b), \quad \varphi(1) = 1.$$

Ist φ zudem bijektiv, so nennen wir φ einen **Isomorphismus** (G1P).

Beispiele: Die Inklusionen $\mathbb{Z} \hookrightarrow \mathbb{Q} \hookrightarrow \mathbb{R} \hookrightarrow \mathbb{C} \hookrightarrow \mathbb{H}$ sind Ringhomomorphismen, ebenso die Quotientenabbildung $\mathbb{Z} \twoheadrightarrow \mathbb{Z}/n\mathbb{Z}$.

Beispiel: Die Konjugation $\bar{\cdot} : \mathbb{C} \rightarrow \mathbb{C} : x + iy \mapsto x - iy$ erfüllt $\overline{\bar{z}} = z$ sowie $\overline{z + w} = \bar{z} + \bar{w}$ und $\overline{z \cdot w} = \bar{z} \cdot \bar{w}$, ist also ein Automorphismus (A3B).

Beispiel: Die Abbildung $\varphi : \mathbb{Z} \rightarrow \mathbb{Z} : a \mapsto 0$ ist additiv und multiplikativ, erfüllt aber nicht $\varphi(1) = 1$. Somit ist φ kein Ringhomomorphismus.

Lemma G2F: Komposition und Umkehrung

- (0) Für jeden Ring $(R, +, 0, \cdot, 1)$ ist $\text{id}_R: R \rightarrow R$ ein Homomorphismus.
- (1) Ist $\varphi: (R, +, 0, \cdot, 1) \rightarrow (S, +, 0, \cdot, 1)$ und $\psi: (S, +, 0, \cdot, 1) \rightarrow (T, +, 0, \cdot, 1)$ ein Homomorphismus, so auch $\psi \circ \varphi: (R, +, 0, \cdot, 1) \rightarrow (T, +, 0, \cdot, 1)$.
- (2) Ist $\varphi: (R, +, 0, \cdot, 1) \rightarrow (S, +, 0, \cdot, 1)$ ein bijektiver Homomorphismus, so auch $\psi = \varphi^{-1}: (S, +, 0, \cdot, 1) \rightarrow (R, +, 0, \cdot, 1)$.

Aufgabe: Beweisen Sie dies zur Wiederholung (G1P).

Unterringe und Unterkörper

Definition G2G: Unterring und Unterkörper

Sei $(R, +, 0, \cdot, 1)$ ein Ring und darin $S \subseteq R$ eine Teilmenge.

Wir nennen S einen **Unterring** oder **Teilring**, kurz $S \leq R$, falls gilt:

- 1 $S \leq (R, +, 0)$ ist eine Untergruppe, also $0 \in S$ und $S - S \subseteq S$,
- 2 $S \leq (R, \cdot, 1)$ ein Untermonoid, also $1 \in S$ und $S \cdot S \subseteq S$.

In diesem Falle ist $(S, +_S, 0, \cdot_S, 1)$ selbst ein Ring, und die Inklusion $S \hookrightarrow R$ ist ein Ringhomomorphismus. Ist S zudem ein Körper, so nennen wir S einen **Unterkörper** oder **Teilkörper** in R .

Beispiele: $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C} \subset \mathbb{H}$ sind Teilringe bzw. Teilkörper.

Die Menge $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ ist ein Teilkörper von \mathbb{R} .

Die Menge $\mathbb{Z}[i] \subset \mathbb{C}$ ist ein Teilring, und $\mathbb{Q}[i] \subset \mathbb{C}$ ist ein Teilkörper.

Beispiele: Im Matrixring $\mathbb{R}^{n \times n}$ ist $\mathbb{R} \cdot 1_{n \times n}$ ein Teilkörper.

Auch im Polynomring $\mathbb{R}[X]$ ist $\mathbb{R} \subseteq \mathbb{R}[X]$ ein Teilkörper.

Beispiel: Die Menge $2\mathbb{Z} \subset \mathbb{Z}$ ist kein Teilring, denn $1 \notin 2\mathbb{Z}$.

Der Nullring $\{0\} \subset \mathbb{Z}$ ist kein Teilring von \mathbb{Z} , denn $1 \notin \{0\}$.

Unterringe und Unterkörper

Wir betrachten hier Ringe mit Einselement. Daher verlangen wir von Homomorphismen und Unterringen, dass sie das Einselement erhalten.

Beispiel: Im Ring $(\mathbb{Z}, +, 0, \cdot, 1)$ ist $\{0\}$ eine additive Untergruppe und multiplikativ abgeschlossen. Somit ist $(\{0\}, +, 0, \cdot, 0)$ ein Ring, aber kein Unterring von $(\mathbb{Z}, +, 0, \cdot, 1)$, da das Einselement nicht erhalten bleibt.

Bemerkung: Die Begriffe „Unterring“ und „Teilring“ sind synonym, geschrieben $S \leq R$, so wie „Untermenge“ und „Teilmenge“, $A \subseteq B$.

Im Falle $S \leq R$ nennen wir S einen **Unterring** von R und umgekehrt nennen wir R einen **Oberring** von S oder eine **Ringerweiterung**.

Im Falle $S \subsetneq R$ ist S ein **echter Unterring** von R , geschrieben $S < R$, oder umgekehrt gesagt, R ein **echter Oberring** von S , kurz $R > S$.

Beispiel: Der Körper $\mathbb{C} = \mathbb{R}[i] \supset \mathbb{R}$ der komplexen Zahlen ist eine Körpererweiterung der reellen Zahlen. Gleiches gilt für $\mathbb{Q}[\sqrt{2}] \supset \mathbb{Q}$.

Die Begriffe „Unterkörper“ und „Oberkörper“ klingen zwar recht lustig, entsprechen aber ansonsten genau der Definition für Ringe.

Charakteristischer Unterring

Satz G2H: charakteristischer Unterring und Charakteristik

Zu jedem Ring $(R, +, 0, \cdot, 1)$ existiert genau ein Ringhomomorphismus

$$\varphi : (\mathbb{Z}, +, 0, \cdot, 1) \rightarrow (R, +, 0, \cdot, 1) : k \mapsto k \cdot 1_R = 1_R \cdot k$$

dank Satz G1T. Sein Bild in R ist der **charakteristische Unterring**

$$\text{Char}(R) = \text{Char}(R, +, \cdot) := \{ k \cdot 1_R \mid k \in \mathbb{Z} \}.$$

Für den Kern gilt $\ker(\varphi) := \varphi^{-1}(\{0\}) = n\mathbb{Z}$ für ein $n \in \mathbb{N}$ dank G1v.

Daraus gewinnen wir den charakteristischen **Ringisomorphismus**

$$\bar{\varphi} : \mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} \text{Char}(R) : [k] \mapsto k \cdot 1_R.$$

Wir nennen $\text{char}(R) := n$ die **Charakteristik** des Rings R .

Ist R nullteilerfrei, so ist n prim, also $n \in \{0, 2, 3, 5, 7, 11, 13, \dots\}$.

Beispiele: Für $\mathbb{K} = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{H}$ gilt $\text{Char}(\mathbb{K}) = \mathbb{Z}$ und $\text{char}(\mathbb{K}) = 0$.

Für $R = \mathbb{Z}/n, (\mathbb{Z}/n)[X], (\mathbb{Z}/n)^{s \times s}$ gilt $\text{Char}(R) \cong \mathbb{Z}/n$ und $\text{char}(R) = n$.

Charakteristischer Unterring

Anschaulich entsteht die Menge $\text{Char}(R)$ aus dem Einselement 1 durch wiederholte Addition bzw. Subtraktion. Die elegantere Sichtweise ist der eindeutige Ringhomomorphismus $\varphi: \mathbb{Z} \rightarrow R$ mit Bild $\text{im}(\varphi) = \text{Char}(R)$.

Bemerkung: Somit ist $\text{Char}(R)$ der kleinste Teilring von $(R, +, 0, \cdot, 1)$, denn jeder Teilring $S \leq (R, +, 0, \cdot, 1)$ enthält 1 und somit $\text{Char}(R)$.

😊 In jedem noch so komplizierten Ring R finden wir einen sehr vertrauten Unterring $\mathbb{Z}/n\mathbb{Z} \cong \text{Char}(R)$ dank des Isomorphismus $\bar{\varphi}$.

Freshman's dream: Frobenius–Endomorphismus

Im Allgemeinen gilt $(a + b)^2 = a^2 + 2ab + b^2 \neq a^2 + b^2$.

In Charakteristik 2 gilt $1 + 1 = 0$, also sind beide gleich!

Satz G2I: Frobenius–Endomorphismus in Charakteristik p

Sei $(R, +, \cdot)$ ein kommutativer Ring von Primcharakteristik $p > 0$.

Dann ist die Abbildung

$$f = f_R : (R, +, \cdot) \rightarrow (R, +, \cdot) : a \mapsto a^p$$

ein Ringhomomorphismus, genannt **Frobenius–Endomorphismus**.

Beweis: Es gilt $f(a \cdot b) = (a \cdot b)^p = a^p \cdot b^p = f(a) \cdot f(b)$ sowie $f(1) = 1$.

Die Addition ist interessant: Für alle $k \in \mathbb{N}$ mit $0 < k < p$ gilt

$$\binom{p}{k} = \frac{p(p-1) \cdots (p-k+1)}{k(k-1) \cdots 1} \in p\mathbb{Z},$$

denn die Primzahl p erscheint nur im Zähler, aber nicht im Nenner (A2J).

Dank G2D folgt $f(a + b) = \sum_{k=0}^p \binom{p}{k} a^k b^{p-k} = a^p + b^p = f(a) + f(b)$. QED

Freshman's dream: Frobenius–Endomorphismus

Beide Voraussetzungen des Satzes sind wesentlich: Primcharakteristik und Kommutativität. Hierzu ein einfaches, aber illustratives Beispiel:

Aufgabe: Sei $p \geq 2$ prim. In $\mathbb{Z}_p^{2 \times 2}$ betrachten wir die Matrizen

$$E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \quad C = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Berechnen Sie A^n und B^n sowie $(E + A)^n$ und $(E + B)^n$ für $n \in \mathbb{N}$. Für welche Exponenten $n \in \mathbb{N}$ gilt demnach $(E + A)^n = E^n + A^n$? Vergleichen Sie $(A + B)^n$ mit $A^n + B^n$: Wann gilt hier Gleichheit?

Lösung: Es gilt $A^0 = B^0 = E$ und $A^n = B^n = 0$ für $n \geq 2$.

Dank $EA = AE$ gilt $(E + A)^n = \sum_{k=0}^n \binom{n}{k} E^{n-k} A^k = E + nA$.

Für alle Exponenten $n \geq 2$ gilt andererseits $E^n + A^n = E$.

Also gilt $(E + A)^n = E^n + A^n$ genau dann, wenn $n \in \{1\} \cup p\mathbb{N}_{\geq 1}$.

Es gilt $A + B = C$ und $C^n = E$ für n gerade und $C^n = C$ für n ungerade.

Hingegen gilt $A^n + B^n = 0$ für $n \geq 2$, also $(A + B)^n = A^n + B^n$ für $n = 1$, aber nicht für $n \neq 1$. Selbst für $n = p$ gilt hier $(A + B)^p \neq A^p + B^p$.

Beispiel: Matrixringe

◆ Satz B1A: Matrixring über R

Sei $(R, +, 0, \cdot, 1)$ ein Ring und $n \in \mathbb{N}_{\geq 1}$ eine natürliche Zahl.

Die $n \times n$ -Matrizen über R bilden den Ring $(R^{n \times n}, \mathbf{+}, 0_{n \times n}, \cdot, 1_{n \times n})$:

$$\mathbf{+} : R^{n \times n} \times R^{n \times n} \rightarrow R^{n \times n} : (A, B) \mapsto C = A \mathbf{+} B, \quad c_{ij} = a_{ij} + b_{ij},$$

$$\cdot : R^{n \times n} \times R^{n \times n} \rightarrow R^{n \times n} : (A, B) \mapsto C = A \cdot B, \quad c_{ik} = \sum_{j=1}^n a_{ij} \cdot b_{jk}.$$

Für $n \geq 2$ ist dieser Matrixring nicht kommutativ und hat Nullteiler:

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \quad \text{vs} \quad \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

In $R^{n \times n}$ liegt der Unterring $R \cdot 1_{n \times n} = \{ \text{diag}(a, \dots, a) \mid a \in R \}$.

Dieser ist isomorph zum Koeffizientenring R dank der Einbettung

$$\varphi : R \xrightarrow{\sim} R \cdot 1_{n \times n} : a \mapsto a \cdot 1_{n \times n}.$$

Für die Charakteristik gilt demnach $\text{char}(R^{n \times n}) = \text{char}(R)$.

Beispiel: Matrixringe

◆ Beispiel B1F: die komplexen Zahlen \mathbb{C} als Matrizen über \mathbb{R}

Im Matrixring $(\mathbb{R}^{2 \times 2}, +, 0_{2 \times 2}, \cdot, 1_{2 \times 2})$ ist die Teilmenge

$$C := \left\{ z = \begin{bmatrix} x & -y \\ y & x \end{bmatrix} \mid x, y \in \mathbb{R} \right\}$$

ein Unterkörper isomorph zu den komplexen Zahlen A3B:

$$(\mathbb{C}, +, \cdot) \cong (C, +, \cdot) : x + iy \mapsto \begin{bmatrix} x & -y \\ y & x \end{bmatrix}$$

◆ Beispiel B1G: die Quaternionen \mathbb{H} als Matrizen über \mathbb{C}

Im Matrixring $(\mathbb{C}^{2 \times 2}, +, 0_{2 \times 2}, \cdot, 1_{2 \times 2})$ ist die Teilmenge

$$H := \left\{ q = \begin{bmatrix} z & -w \\ w & \bar{z} \end{bmatrix} \mid z, w \in \mathbb{C} \right\} = \mathbb{R}E + \mathbb{R}I + \mathbb{R}J + \mathbb{R}K$$

$$\text{mit } E = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, I = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, J = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, K = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

ein Divisionsring isomorph zu Hamiltons Quaternionen A3D:

$$(\mathbb{H}, +, \cdot) \cong (H, +, \cdot) : \alpha + \beta i + \gamma j + \delta k \mapsto \alpha E + \beta I + \gamma J + \delta K$$

Beispiel: Transposition

😊 Die Konstruktion von $C < \mathbb{R}^{2 \times 2}$ und $H < \mathbb{C}^{2 \times 2}$ als Teilring ist eine enorme Arbeitersparnis: Den Matrixring $K^{n \times n}$ über einem Ring K haben wir bereits allgemein konstruiert. Für C und H genügt dann die Prüfung der (wenigen!) Axiome eines Unterringes bzw. Unterkörpers!

Beispiel G2J: Transposition

Sei $(K, +, \cdot)$ ein kommutativer Ring. Dann ist die Transposition

$$\tau : K^{n \times n} \rightarrow K^{n \times n} : A \mapsto A^\tau$$

ein Anti-Automorphismus: Statt Multiplikativität gilt entgegengesetzt

$$(A \cdot B)^\tau = B^\tau \cdot A^\tau.$$

Beweis: Wir setzen die Definitionen ein und rechnen es nach:

$$\begin{aligned} (A \cdot B)_{ki}^\tau &= (A \cdot B)_{ik} &= \sum_{j=1}^n a_{ij} \cdot b_{jk} \\ (B^\tau \cdot A^\tau)_{ki} &= \sum_{j=1}^n b_{kj}^\tau \cdot a_{ji}^\tau &= \sum_{j=1}^n b_{jk} \cdot a_{ij} \end{aligned}$$

Additivität $(A + B)^\tau = A^\tau + B^\tau$ und Involution $(A^\tau)^\tau = A$ sind klar. QED

Beispiel: Transposition-Konjugation

Beispiel G2k: Transposition-Konjugation

Sei $(R, +, \cdot)$ ein Ring und $*$: $R \rightarrow R : a \mapsto a^*$ ein Anti-Automorphismus. Zu $A = (a_{ij})_{ij}$ ist dann $A^\dagger = (a_{ij}^*)_{ji}$ die transponiert-konjugierte Matrix.

Dies definiert einen Anti-Automorphismus $\dagger : R^{n \times n} \rightarrow R^{n \times n} : A \mapsto A^\dagger$. Statt Multiplikativität gilt entgegengesetzt $(A \cdot B)^\dagger = B^\dagger \cdot A^\dagger$.

Beweis: Wir setzen die Definitionen ein und rechnen es nach:

$$\begin{aligned} (A \cdot B)_{ki}^\dagger &= (A \cdot B)_{ik}^* &&= \sum_{j=1}^n (a_{ij} \cdot b_{jk})^* \\ (B^\dagger \cdot A^\dagger)_{ki} &= \sum_{j=1}^n (B^\dagger)_{kj} \cdot (A^\dagger)_{ji} &&= \sum_{j=1}^n b_{jk}^* \cdot a_{ij}^* \end{aligned}$$

Additivität $(A + B)^\dagger = A^\dagger + B^\dagger$ und Involution $(A^\dagger)^\dagger = A$ sind klar. QED

Beispiele: Auf $\mathbb{K} = \mathbb{R}, \mathbb{C}, \mathbb{H}$ mit der Konjugation $a \mapsto a^* = \bar{a}$ erhalten wir den Anti-Automorphismus $\dagger : \mathbb{K}^{n \times n} \rightarrow \mathbb{K}^{n \times n} : A \mapsto A^\dagger = \overline{A}^\top$. Speziell auf $C < \mathbb{R}^{2 \times 2}$ ist $z = \begin{bmatrix} x & -y \\ y & x \end{bmatrix} \mapsto z^\top = \begin{bmatrix} x & y \\ -y & x \end{bmatrix}$ die komplexe Konjugation (B1F). Auf $H < \mathbb{C}^{2 \times 2}$ ist $q \mapsto q^\dagger = \bar{q}^\top$ die quaternionische Konjugation (B1G).

Zentrum eines Rings

Zwei Elemente a, b im Ring R **kommutieren**, falls $ab = ba$ gilt.
Anders gesagt, ihr **Kommutator** $[a, b] := ab - ba$ ist gleich Null.

Das **Zentrum** des Rings $(R, +, 0, \cdot, 1)$ ist die Menge

$$Z(R) = Z(R, \cdot) = \{ z \in R \mid \forall a \in R: az = za \}.$$

Anders gesagt, ein Element $z \in R$ ist **zentral** im Ring R , falls z mit allen Elementen $a \in R$ kommutiert.

Satz G2L: Das Zentrum ist ein Unterring.

Das Zentrum $Z(R)$ ist ein kommutativer Unterring von $(R, +, 0, \cdot, 1)$.
Ist R zudem ein Divisionsring, so ist $Z(R)$ ein Unterkörper.

Beispiele: Genau dann gilt $Z(R) = R$, wenn R kommutativ ist.

Im Ring \mathbb{H} der Quaternionen finden wir das Zentrum $Z(\mathbb{H}) = \mathbb{R}$.

Es gilt $Z(R^{n \times n}) = Z(R) \cdot 1_{n \times n} = \{ \text{diag}(a, \dots, a) \mid a \in Z(R) \}$.

Zentrum eines Rings

Aufgabe: Rechnen Sie die Aussage des Satzes nach. Was ist zu tun?

Kartesisches Produkt mit koordinatenweiser Verknüpfung

Beispiel G2M: Produkt $R_1 \times \cdots \times R_n$ von Ringen

Ist $(R_i, +_i, 0_i, \cdot_i, 1_i)$ ein Ring für $i = 1, \dots, n$, so auch

$$\begin{aligned} (R, +, 0, \cdot, 1) \quad \text{mit} \quad R = R_1 \times \cdots \times R_n \quad \text{und} \\ (a_1, \dots, a_n) + (b_1, \dots, b_n) &= (a_1 +_1 b_1, \dots, a_n +_n b_n), \\ (a_1, \dots, a_n) \cdot (b_1, \dots, b_n) &= (a_1 \cdot_1 b_1, \dots, a_n \cdot_n b_n), \\ \text{sowie} \quad 0 &= (0_1, \dots, 0_n) \quad \text{und} \quad 1 = (1_1, \dots, 1_n). \end{aligned}$$

Die Projektion $\text{pr}_i: R \rightarrow R_i: a \mapsto a_i$ ist ein Ringhomomorphismus, i.A. aber nicht die Einbettung $\iota_i: R_i \hookrightarrow R: a_i \mapsto (0_1, \dots, a_i, \dots, 0_n)$.

Für das Zentrum gilt $Z(R_1 \times \cdots \times R_n) = Z(R_1) \times \cdots \times Z(R_n)$.

Für $n \geq 2$ hat R Nullteiler, $(1, 0, 0, \dots) \cdot (0, 1, 0, \dots) = (0, 0, 0, \dots)$.

Beweis: Geduldiges Nachrechnen (G1x). Übung!

◻

Beispiel: Im Ring $R^{n \times n}$ ist $D = \{ \text{diag}(a_1, \dots, a_n) \mid a_1, \dots, a_n \in R \}$ ein Teilring isomorph zum Produktring $R^n = R \times \cdots \times R$.

Funktionen mit punktweiser Verknüpfung

Beispiel: Die reellen Funktionen $f: \mathbb{R}^n \supseteq \Omega \rightarrow \mathbb{R}$ bilden einen Ring bezüglich punktweiser Addition und Multiplikation. Ausführlich:

Beispiel G2N: Potenz R^Ω eines Rings, Funktionenring

Sei Ω eine Menge. Ist $(R, +, \cdot)$ ein Ring, so auch die Potenz

$$(R, +, \cdot)^\Omega = (R^\Omega, \boldsymbol{+}, \cdot) \text{ mit } R^\Omega = \text{Abb}(\Omega, R) = \{ f: \Omega \rightarrow R \},$$

$$(f \boldsymbol{+} g)(x) = f(x) + g(x) \text{ und } (f \cdot g)(x) = f(x) \cdot g(x)$$

Hierbei ist $\text{pr}_x: R^\Omega \rightarrow R: f \mapsto f(x)$ ein Ringhomomorphismus, i.A. aber nicht $\iota_x: R \hookrightarrow R^\Omega: a \mapsto f$ mit $f(x) = a$ und $f(y) = 0$ für $y \neq x$.

Für das Zentrum gilt $Z(R^\Omega) = Z(R)^\Omega$. Für $\#\Omega \geq 2$ hat R^Ω Nullteiler.

In R^Ω liegen die Funktionen mit endlichem Träger, $R^{(\Omega)} \subseteq R^\Omega$.

Im Falle $\#\Omega = \infty$ ist $R^{(\Omega)}$ ein „Teilring ohne Eins“.

Beweis: Geduldiges Nachrechnen (G1Y). Übung!

□

Beispiel: Wir erhalten so den Funktionenring $\mathbb{R}^\mathbb{R} = \{ f: \mathbb{R} \rightarrow \mathbb{R} \}$, allgemein den Funktionenring R^R für jeden Ring $(R, +, 0, \cdot, 1)$.

Polynomringe: Definition

Definition G3A: Polynomring $K[X]$ über K in einer Variablen X
 Sei $(R, +, 0, \cdot, 1)$ ein kommutativer Ring, $K \leq R$ ein Teilring und $X \in R$.
 Wir nennen R einen **Polynomring** über dem Koeffizientenring $K \leq R$ in der Variablen $X \in R$, geschrieben $R = K[X]$, falls sich jedes Element $P \in R^*$ eindeutig schreiben lässt als eine Summe der Form

$$P = p_0 + p_1X + p_2X^2 + \cdots + p_nX^n$$

mit $n \in \mathbb{N}$ und $p_0, p_1, p_2, \dots, p_n \in K$ sowie $p_n \neq 0$. Wir nennen P dann ein **Polynom** vom **Grad** $\deg(P) := n$ mit **Leitkoeffizient** $\text{lc}(P) := p_n$.

Dabei heißt X^i das ***i*te Monom** in X und p_i der ***i*te Koeffizient** sowie p_iX^i der ***i*te Term** des Polynoms P . Wir schreiben kurz

$$P = \sum_{i=0}^n p_i X^i = \sum_{i \in \mathbb{N}} p_i X^i = \sum_i p_i X^i$$

und vereinbaren dazu $p_i = 0$ für alle $i > n$.

Für das **Nullpolynom** $P = 0$ setzen wir $\deg(0) := -\infty$ und $\text{lc}(0) := 0$.

Polynomringe: Addition und Multiplikation

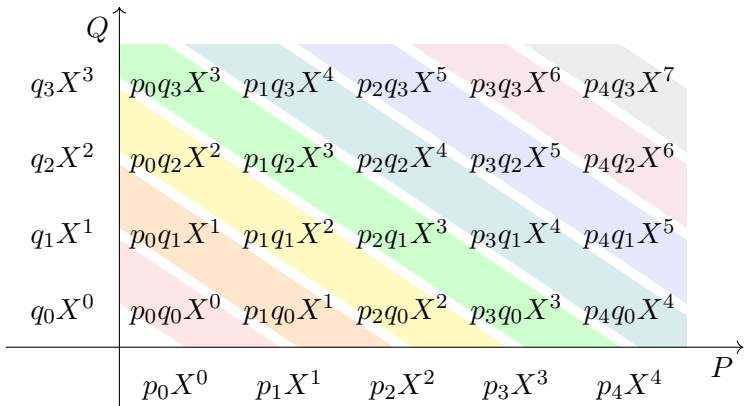
Die raffinierte Definition G3A impliziert sofort folgende Rechenregeln:

Vergleich: $\sum_i p_i X^i = \sum_i q_i X^i$ in $K[X] \Leftrightarrow p_i = q_i$ in K für alle i

Addition: $[\sum_i p_i X^i] + [\sum_i q_i X^i] = \sum_i (p_i + q_i) X^i$

Multiplikation: $[\sum_i p_i X^i] \cdot [\sum_j q_j X^j] = \sum_k r_k X^k, r_k = \sum_{i+j=k} p_i q_j$

Diese (endliche!) Summe durchläuft alle Paare $(i, j) \in \mathbb{N}^2$ mit $i + j = k$.



Rechenregeln für den Polynomgrad

Satz G3B: Rechenregeln für den Polynomgrad

(1) Für je zwei Polynome P und Q in $K[X]$ gilt:

$$\deg(P + Q) \leq \max\{\deg P, \deg Q\}$$

Gleichheit gilt genau dann, wenn $\deg P \neq \deg Q$ oder $\text{lc } P + \text{lc } Q \neq 0$.

(2) Für je zwei Polynome P und Q in $K[X]$ gilt:

$$\deg(P \cdot Q) \leq \deg P + \deg Q$$

Gleichheit gilt genau dann, wenn $P = 0$ oder $Q = 0$ oder $\text{lc } P \cdot \text{lc } Q \neq 0$.
In diesem Fall gilt für die Leitkoeffizienten $\text{lc}(P \cdot Q) = \text{lc } P \cdot \text{lc } Q$.

(3) Genau dann ist $K[X]$ ein Integritätsring, wenn K dies ist. Dann gilt:

$$\begin{aligned}\deg(P \cdot Q) &= \deg(P) + \deg(Q) \\ \text{lc}(P \cdot Q) &= \text{lc}(P) \cdot \text{lc}(Q)\end{aligned}$$

Rechenregeln für den Polynomgrad

Beweis: (1,2) Die beiden Ungleichungen sind klar. Die Bedingungen für Gleichheit folgen aus obigen Formeln für Addition und Multiplikation.

(3) „ \Rightarrow “: Ist $K[X]$ nullteilerfrei, so auch der Unterring K .

„ \Leftarrow “: Ist K nullteilerfrei, so auch $K[X]$ dank (2). QED

Beispiel: Wider Erwarten gilt nicht immer $\deg(PQ) = \deg P + \deg Q$.

In $\mathbb{Z}/6\mathbb{Z}[X]$ gilt $(\bar{1} + \bar{2}X) \cdot (\bar{1} + \bar{3}X) = \bar{1} + \bar{5}X + \bar{6}X^2 = \bar{1} + \bar{5}X$.

In $\mathbb{Z}/4\mathbb{Z}[X]$ gilt $(\bar{1} + \bar{2}X) \cdot (\bar{1} + \bar{2}X) = \bar{1} + \bar{4}X + \bar{4}X^2 = \bar{1}$.

😊 Über einem Integritätsring kann dieses Problem nicht auftreten!

Aufgabe: Für jeden Integritätsring K gilt $K[X]^\times = K^\times$.

Lösung: Die Inklusion $K[X]^\times \supseteq K^\times$ ist klar. Wir zeigen $K[X]^\times \subseteq K^\times$:
Für $P, Q \in K[X]$ mit $PQ = 1$ gilt $0 = \deg 1 = \deg(PQ) = \deg P + \deg Q$
dank (2), also $\deg P = \deg Q = 0$, somit $P, Q \in K^\times$.

Beispiele und Gegenbeispiele

Aufgabe: Für $S = \mathbb{Q}[\sqrt{2}] := \{ a + b\sqrt{2} \mid a, b \in \mathbb{Q} \}$ gilt $\mathbb{Q} < S < \mathbb{R}$.
Ist S ein Polynomring über $\mathbb{Q} \leq S$ in der Variablen $x = \sqrt{2}$?

Lösung: Nein! Jedes Element $p \in S$ schreibt sich zwar als eine Summe $p = \sum_k p_k x^k$ mit $p_k \in \mathbb{Q}$, aber nicht eindeutig: $2x^0 - 1x^2 = 0$.

Aufgabe: Für $T = \mathbb{Q}[e] := \{ \sum_k p_k e^k \mid p_k \in \mathbb{Q} \}$ gilt $\mathbb{Q} < T < \mathbb{R}$.
Ist T ein Polynomring über $\mathbb{Q} \leq T$ in der Variablen $x = e$?

Lösung: Ja! Jedes Element $p \in T$ schreibt sich als eine Summe $p = \sum_k p_k x^k$ mit $p_k \in \mathbb{Q}$, aber zwar eindeutig, denn e ist transzendent.

Aufgabe: Ist \mathbb{R} ein Polynomring über $\mathbb{Q} \leq \mathbb{R}$ in einer Variablen $x \in \mathbb{R}$?

Lösung: Nein! Nicht jede reelle Zahl $r \in \mathbb{R}$ schreibt sich als Summe $r = \sum_k r_k x^k$ mit $r_k \in \mathbb{Q}$: Die Menge $\mathbb{Q}[x] = \bigcup_{n \in \mathbb{N}} \{ \sum_{k=0}^{n-1} p_k x^k \mid p_k \in \mathbb{Q} \}$ ist abzählbar (F2L), aber die gesamte Menge \mathbb{R} ist überabzählbar (F2R).

😊 Bitte lesen Sie noch einmal sorgfältig die raffinierte Definition G3A.
Diese Beispiele illustrieren eindrücklich ihre Flexibilität und Präzision.

Normierte Polynome

Ein Polynom $P \in K[X]$ heißt **normiert**, falls $\text{lc}(P) = 1$ gilt.

$$K[X]_n^1 = \{ P \in K[X] \mid \deg P = n \wedge \text{lc} P = 1 \}$$

$$K[X]_n = \{ P \in K[X] \mid \deg P = n \}$$

$$K[X]_{\leq n} = \{ P \in K[X] \mid \deg P \leq n \}$$

$$K[X]_{< n} = \{ P \in K[X] \mid \deg P < n \}$$

Durch Einschränkung erhalten wir folgende Verknüpfungen:

$$+ : K[X]_{\leq n} \times K[X]_{\leq n} \rightarrow K[X]_{\leq n}$$

$$\cdot : K[X]_{\leq r} \times K[X]_{\leq s} \rightarrow K[X]_{\leq r+s}$$

Normierung verhindert Auslöschung im höchsten Grad:

$$\cdot : K[X]_r^1 \times K[X]_s^1 \rightarrow K[X]_{r+s}^1$$

$$\cdot : K[X]_r^1 \times K[X]_s \rightarrow K[X]_{r+s}$$

$$\cdot : K[X]_r \times K[X]_s^1 \rightarrow K[X]_{r+s}$$

Polynom und Polynomfunktion


Definition G3C: Jedes Polynom definiert eine Polynomfunktion.

Jedes Polynom $P(X) = \sum_{i=0}^n p_i X^i$ in $K[X]$ definiert eine Funktion

$$f_P : K \rightarrow K : a \mapsto P(a) = \sum_{i=0}^n p_i a^i.$$

Wir nennen f_P die **Polynomfunktion** des Polynoms P .

Beispiel: Für $P = X^2 + X \in \mathbb{Z}_2[X]$ gilt $P(0) = P(1) = 0$, also $f_P = 0$.

 Für das Polynom gilt $P \neq 0$, und dennoch $f_P = 0$. Wir unterscheiden sorgsam zwischen Polynom $P \in K[X]$ und Funktion $f_P : K \rightarrow K$.

Definition G3C: Polynomfunktion für Matrizen (Fortsetzung)

Ebenso können wir in $P(X)$ eine quadratische Matrix einsetzen:

$$F_P : K^{m \times m} \rightarrow K^{m \times m} : A \mapsto P(A) = \sum_{i=0}^n p_i A^i.$$

Beispiel: Für $A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \in \mathbb{Z}_2^{2 \times 2}$ gilt $P(A) = A^2 + A = 0 + A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$.

Satz G3D: Polynom und Polynomfunktion

Weiterhin sei $(K, +, \cdot)$ ein kommutativer Ring. Die Zuordnung

$$f : K[X] \rightarrow \text{Abb}(K, K) : P \mapsto f_P$$

ist ein Ringhomomorphismus (siehe G2N). Das heißt ausführlich:

Es gilt $f_0 = 0$ und $f_{P+Q} = f_P + f_Q$ sowie $f_1 = 1$ und $f_{P \cdot Q} = f_P \cdot f_Q$.

Dasselbe gilt entsprechend für Matrizen:

$$F : K[X] \rightarrow \text{Abb}(K^{m \times m}, K^{m \times m}) : P \mapsto F_P$$

Übung: Rechnen Sie die Eigenschaften sorgsam nach:

$$\begin{aligned} f_{P+Q}(a) &\stackrel{\text{Def}}{=} (P+Q)(a) \stackrel{!}{=} P(a) + Q(a) \stackrel{\text{Def}}{=} f_P(a) + f_Q(a) \\ f_{P \cdot Q}(a) &\stackrel{\text{Def}}{=} (P \cdot Q)(a) \stackrel{!}{=} P(a) \cdot Q(a) \stackrel{\text{Def}}{=} f_P(a) \cdot f_Q(a) \end{aligned}$$

😊 Diese Beispiele sind Spezialfälle des folgenden Satzes.

Satz G3E: universelle Abbildungseigenschaft (UAE)

Sei $(K, +, \cdot)$ ein kommutativer Ring und $(R, +, \cdot)$ ein Ring sowie $\varphi: K \rightarrow R$ ein Ringhomomorphismus mit $\varphi(K) \subseteq Z(R)$.

$$\begin{array}{ccccc}
 K & \xrightarrow{\text{inc}} & K[X] & \xleftarrow{\text{inc}} & \{X\} \\
 & \searrow \text{zentral} & \downarrow \exists! \Phi & \swarrow a \mapsto X & \\
 & \varphi & R & &
 \end{array}$$

Zu jedem Element $a \in R$ existiert genau einen Ringhomomorphismus $\Phi: K[X] \rightarrow R$ mit $\Phi|_K = \varphi$ und $\Phi(X) = a$. Dieser ist gegeben durch

$$\Phi(p_0 + p_1X + \cdots + p_nX^n) = \varphi(p_0) + \varphi(p_1)a + \cdots + \varphi(p_n)a^n.$$

Wir nennen $\Phi = \Phi_a = \Phi_{X \mapsto a}$ den **Einsetzungshomomorphismus**.

Die universelle Abbildungseigenschaft des Polynomrings

Eindeutigkeit: Sind $\Phi, \Psi : K[X] \rightarrow R$ zwei Ringhomomorphismen mit $\Phi|_K = \Psi|_K = \varphi$ und $\Phi(X) = \Psi(X) = a$, so gilt $\Phi = \Psi$, denn:

$$\Phi\left(\sum_i p_i X^i\right) \stackrel{\text{add}}{=} \sum_i \Phi(p_i X^i) \stackrel{\text{mult}}{=} \sum_i \Phi(p_i) \Phi(X)^i \stackrel{\varphi}{\underset{X \mapsto a}{=}} \sum_i \varphi(p_i) a^i$$

$$\Psi\left(\sum_i p_i X^i\right) \stackrel{\text{add}}{=} \sum_i \Psi(p_i X^i) \stackrel{\text{mult}}{=} \sum_i \Psi(p_i) \Psi(X)^i \stackrel{\varphi}{\underset{X \mapsto a}{=}} \sum_i \varphi(p_i) a^i$$

Das beweist die Eindeutigkeit und gibt uns auch schon einen Hinweis, wie wir die ersehnte Abbildung $\Phi : K[X] \rightarrow R$ konstruieren müssen:

Existenz: Wir konstruieren $\Phi : K[X] \rightarrow R$ wie folgt: Jedes Element $P \in K[X]$ schreibt sich nach Definition G3A eindeutig als Summe $P = \sum_i p_i X^i$ mit $p_i \in K$. Wir setzen dann $\Phi(P) := \sum_i \varphi(p_i) a^i$.

Homomorphie: Damit ist die Eindeutigkeit gezeigt und die (einzig mögliche) Abbildung $\Phi : K[X] \rightarrow R$ konstruiert. Es bleibt nun noch nachzuweisen, dass Φ tatsächlich ein Ringhomomorphismus ist.

Die universelle Abbildungseigenschaft des Polynomrings

Es gilt $\Phi(0) = \varphi(0) = 0$ und $\Phi(1) = \varphi(1) = 1$.

Für die Addition finden wir:

$$\begin{aligned}\Phi([\sum_i p_i X^i] + [\sum_i q_i X^i]) &= \Phi(\sum_i [p_i + q_i] X^i) \\ &= \sum_i \varphi(p_i + q_i) a^i\end{aligned}$$

$$\begin{aligned}\Phi(\sum_i p_i X^i) + \Phi(\sum_i q_i X^i) &= [\sum_i \varphi(p_i) a^i] + [\sum_i \varphi(q_i) a^i] \\ &= \sum_i [\varphi(p_i) + \varphi(q_i)] a^i\end{aligned}$$

Für die Multiplikation finden wir entsprechend:

$$\begin{aligned}\Phi([\sum_i p_i X^i] \cdot [\sum_j q_j X^j]) &= \Phi(\sum_k [\sum_{i+j=k} p_i q_j] X^k) \\ &= \sum_k [\sum_{i+j=k} \varphi(p_i q_j)] a^k\end{aligned}$$

$$\begin{aligned}\Phi(\sum_i p_i X^i) \cdot \Phi(\sum_j q_j X^j) &= [\sum_i \varphi(p_i) a^i] \cdot [\sum_j \varphi(q_j) a^j] \\ &= \sum_k [\sum_{i+j=k} \varphi(p_i) \varphi(q_j)] a^k\end{aligned}$$

Hier nutzen wir, dass alle $b \in \varphi(K)$ mit $a \in R$ kommutieren.

QED

Die universelle Abbildungseigenschaft des Polynomrings

Diese sorgsame Rechnung ist länglich, aber nicht wirklich schwer. So ist es oft bei grundlegenden Überprüfungen: Ihre Ausführung ist nahezu mechanisch, aber auch dies muss erledigt werden.

Wir sehen dabei kleinste Details, die sonst leicht übersehen werden, hier dass a mit allen Koeffizienten $b \in \varphi(K)$ kommutieren muss. Genau dazu dient die technische Voraussetzung $\varphi(K) \leq Z(R)$.

Auch dies ist ein allgemeines Phänomen: Durch die Ausführung des Beweises verstehen Sie den Satz wesentlich besser, Voraussetzung und Folgerung! Und Sie sehen, dass der Beweis gar nicht schwer ist.

Das Gegenstück hierzu sind gute Beispiele und Gegenbeispiele. Diesen wenden wir uns nun anschließend zu.

Erste Anwendungen der universellen Abbildungseigenschaft

Dank UAE (Satz G3E) haben wir die Ring-Endomorphismen

$$F_p : K[X] \rightarrow K[X] : X \mapsto X^p \quad \text{für } p \in \mathbb{N},$$

wobei stillschweigend $F_p|_K = \text{id}_K$ gelte.

Aufgabe: Es gilt $F_1 = \text{id}_{K[X]}$ und $F_p \circ F_q = F_{p \cdot q}$ für alle $p, q \in \mathbb{N}$.

Lösung: Dank Eindeutigkeit gilt $F_1 = \text{id}_{K[X]}$ und $F_p \circ F_q = F_{pq}$:

$$(F_p \circ F_q)(X) = F_p(F_q(X)) = F_p(X^q) = (X^p)^q = X^{pq} = F_{pq}(X).$$

Ausführlich: Beide Abbildungen $F_p \circ F_q$ und F_{pq} sind Endomorphismen des Rings $K[X]$, eingeschränkt auf K sind beide die Identität, und beide bilden die Variable X gleich ab, denn $(F_p \circ F_q)(X) = F_{pq}(X)$.

Dank der Eindeutigkeitsaussage von Satz G3E folgt $F_p \circ F_q = F_{p \cdot q}$.

Erste Anwendungen der universellen Abbildungseigenschaft

Dank UAE (Satz G3E) haben wir die Ring-Endomorphismen

$$G_a : K[X] \rightarrow K[X] : X \mapsto X + a \quad \text{für } a \in K,$$

wobei stillschweigend $G_a|_K = \text{id}_K$ gelte.

Aufgabe: Es gilt $G_0 = \text{id}_{K[X]}$ und $G_a \circ G_b = G_{a+b}$ für alle $a, b \in K$.

Lösung: Dank Eindeutigkeit gilt $G_0 = \text{id}_{K[X]}$ und $G_a \circ G_b = G_{a+b}$:

$$\begin{aligned} (G_a \circ G_b)(X) &= G_a(G_b(X)) = G_a(X + b) = (X + a) + b \\ &= X + (a + b) = G_{a+b}(X). \end{aligned}$$

Beide Abbildungen $G_a \circ G_b$ und G_{a+b} sind Endomorphismen des Rings $K[X]$, eingeschränkt auf K sind beide die Identität, und beide bilden die Variable X auf dasselbe Element ab, denn $(G_a \circ G_b)(X) = G_{a+b}(X)$.

Dank der Eindeutigkeitsaussage von Satz G3E folgt $G_a \circ G_b = G_{a+b}$.

Insbesondere gilt demnach $G_a \circ G_{-a} = G_{a-a} = G_0 = \text{id}_{K[X]}$.

Somit ist G_a ein Ringautomorphismus mit $G_a^{-1} = G_{-a}$.

Eindeutigkeit des Polynomrings bis auf Isomorphismus

Korollar G3F: Eindeutigkeit bis auf Isomorphismus

Je zwei Polynomringe $K[X]$ und $K[Y]$ sind kanonisch isomorph.

Es existiert genau ein Isomorphismus $(\varphi, \psi) : K[X] \cong K[Y]$ mit $\varphi|_K = \psi|_K = \text{id}_K$ sowie $\varphi(X) = Y$ und $\psi(Y) = X$.

Beweis: Dank Satz G3E existiert je genau ein Ringhomomorphismus

$$\varphi : K[X] \rightarrow K[Y] : X \mapsto Y \quad \text{mit} \quad \varphi|_K = \text{id}_K,$$

$$\psi : K[Y] \rightarrow K[X] : Y \mapsto X \quad \text{mit} \quad \psi|_K = \text{id}_K.$$

Dank Eindeutigkeit in G3E gilt $\psi \circ \varphi = \text{id}_{K[X]}$ und $\varphi \circ \psi = \text{id}_{K[Y]}$. QED

Eindeutigkeit des Polynomrings bis auf Isomorphismus

Bemerkung: Erst die Präzisierung $\varphi|_K = \psi|_K = \text{id}_K$ sowie die Wahl $\varphi(X) = Y$ und $\psi(Y) = X$ legen den Isomorphismus (φ, ψ) fest.

Auch $X \mapsto Y + 1$ und $Y \mapsto X - 1$ liefert einen Isomorphismus, wie in der vorigen Aufgabe allgemein ausgeführt.

Auch $\varphi: \mathbb{C}[X] \rightarrow \mathbb{C}[Y]: X \mapsto Y$ mit $\varphi|_{\mathbb{C}} = \text{conj}$ ist ein Isomorphismus; hier werden die Koeffizienten nicht festgehalten, sondern konjugiert.

😊 Satz G3E ist das Universalwerkzeug zur Konstruktion von Ringhomomorphismen $\Phi: K[X] \rightarrow R$ und trägt daher zurecht den klangvollen Namen „universelle Abbildungseigenschaft“, kurz UAE.

Konstruktion des Polynomrings

Satz G3G: Existenz des Polynomrings

Zu jedem kommutativen Ring $(K, +, 0, \cdot, 1)$ existiert ein Polynomring $(K[X], +, 0, \cdot, 1)$.

Beweis: Wir betrachten die Menge

$$R = K^{(\mathbb{N})} = \{ a : \mathbb{N} \rightarrow K : i \mapsto a_i \mid \#\text{supp}(a) < \infty \}$$

der Folgen $a = (a_0, a_1, a_2, \dots)$ mit Werten $a_i \in K$ und endlichem Träger. Das bedeutet, es existiert ein $n \in \mathbb{N}$, sodass $a_i = 0$ für alle $i > n$ gilt. Somit liegt $\deg(p) := \sup\{ n \in \mathbb{N} \mid p_n \neq 0 \}$ in der Menge $\mathbb{N} \cup \{-\infty\}$.

Auf der Menge R definieren wir Summe und Produkt wie oben gesehen:

$$+_R : R \times R \rightarrow R : (a, b) \mapsto s = a +_R b, \quad s_i = a_i + b_i$$

$$\cdot_R : R \times R \rightarrow R : (a, b) \mapsto p = a \cdot_R b, \quad p_k = \sum_{i+j=k} a_i \cdot b_j$$

Man rechnet nun geduldig nach, dass $(R, +_R, 0_R, \cdot_R, 1_R)$ tatsächlich ein kommutativer Ring ist, mit $0_R = (0, 0, 0, \dots)$ und $1_R = (1, 0, 0, \dots)$.

Konstruktion des Polynomrings

😊 Genau so implementieren wir Polynome auf dem Computer. Das so definierte Produkt von Folgen heißt das **Faltungsprodukt**. Es entspricht genau dem Vorbild von Polynomen und tut, was es soll. Die hierzu nötigen Rechnungen sind länglich, aber leicht: Übung! Wir haben die analogen Überprüfungen für Matrizen ausgeführt.

Die Abbildung $\iota: K \rightarrow R: a \mapsto (a, 0, 0, \dots)$ ist ein Ringhomomorphismus und injektiv. Mittels ι identifizieren wir nun den Koeffizientenring K mit dem Teilring $\iota(K) < R$; fortan schreiben wir kurz $K < R$ als Teilring. Statt $(R, +_R, 0_R, \cdot_R, 1_R)$ schreiben wir bequemer $(R, +, 0, \cdot, 1)$.

Speziell für das Element $X = (0, 1, 0, 0, \dots)$ gilt $X^0 = (1, 0, 0, 0, \dots)$, $X^1 = (0, 1, 0, 0, \dots)$, $X^2 = (0, 0, 1, 0, \dots)$, usw. Jedes Element $p \in R$ schreibt sich somit eindeutig als eine (endliche) Summe der Form

$$p = \sum_{i \in \mathbb{N}} p_i X^i.$$

Somit ist R ein Polynomring über $K < R$ in der Variablen X .

◻

Was bedeutet identifizieren?

Es entsteht hier ein kleines, technisches Problem: Wir haben eine Einbettung $\iota: K \hookrightarrow R$, wollen aber eine Teilmenge $K \subseteq R$. Dies tritt immer wieder auf, daher erkläre ich exemplarisch, wie wir dies lösen.

Wir wollen identifizieren vermöge $\iota: K \xrightarrow{\sim} \iota(K) \subseteq R$.

Die einfachste Möglichkeit ist der **Austausch der Elemente**.

Wir nehmen K und R als disjunkt an, wie im obigen Beispiel.

Wir betrachten $R' = (R \setminus \iota(K)) \cup K$, das heißt, wir entfernen die Elemente $\iota(K)$ und ersetzen sie durch K . Wir nutzen die Bijektion $\varphi: R' \xrightarrow{\sim} R$ mit $\varphi(a) = \iota(a)$ für $a \in K$ und $\varphi(b) = b$ für $b \in R \setminus \iota(K)$.

Damit können wir die Ringstruktur von R auf R' verpflanzen, sodass $\varphi: (R', +, \cdot) \xrightarrow{\sim} (R, +, \cdot)$ ein Ringisomorphismus wird:

$$a' + b' := \varphi^{-1}(\varphi(a') + \varphi(b')), \quad a' \cdot b' := \varphi^{-1}(\varphi(a') \cdot \varphi(b'))$$

Die Ringe $(R, +, \cdot)$ und $(R', +, \cdot)$ sind im Wesentlichen gleich, wir haben lediglich die Elemente $\iota(K)$ gegen K ausgetauscht. Nun ist $K \leq R'$ tatsächlich ein Teilring.

Wozu führen wir diese Konstruktion aus?

Polynomringe sind eine grundlegende und allgegenwärtige Konstruktion überall in der Mathematik. Wir üben uns daher in der gebotenen Sorgfalt und erläutern das mathematische Vorgehen im Detail.

Die Definition G3A legt fest, was genau wir von Polynomen verlangen. Die universelle Abbildungseigenschaft G3E garantiert anschließend die Eindeutigkeit des Polynomrings bis auf Isomorphismus G3F.

Eine kritische Leserin muss jedoch befürchten, dass unsere Forderungen gar nicht erfüllbar sind, zumindest nicht immer, etwa weil wir zu viele und widersprüchliche Anforderungen stellen.

Der Satz G3G versichert uns, dass unser Wunsch erfüllbar ist. Wie können wir das beweisen, nachvollziehbar und lückenlos begründen? Die **Existenz** des gewünschten Rings $K[X]$ beweisen wir durch seine **Konstruktion**. Nach Definition G3A ist jedes Polynom $P = \sum_i p_i X^i$ eindeutig durch seine Koeffizientenfolge $p = (p_0, p_1, p_2, \dots) \in K^{(\mathbb{N})}$ festgelegt. Wir können also einfach mit Folgen rechnen. Die Ausführung dieser Idee ist nun leicht, und erfordert lediglich Sorgfalt und Geduld.

Polynome in mehreren Variablen

Genauso konstruiert man den Polynomring in zwei Variablen X, Y :

$$K[X, Y] = \left\{ \sum_{(i,j) \in \mathbb{N}^2} p_{i,j} X^i Y^j \mid p_{i,j} \in K \right\}$$

Dabei gilt $K[X, Y] = K[X][Y] = K[Y][X]$, denn

$$\sum_{(i,j) \in \mathbb{N}^2} p_{i,j} X^i Y^j = \sum_{j \in \mathbb{N}} \left[\sum_{i \in \mathbb{N}} p_{i,j} X^i \right] Y^j = \sum_{i \in \mathbb{N}} \left[\sum_{j \in \mathbb{N}} p_{i,j} Y^j \right] X^i.$$

Auch Polynome in drei Variablen X, Y, Z gelingen ebenso:

$$K[X, Y, Z] = \left\{ \sum_{(i,j,k) \in \mathbb{N}^3} p_{i,j,k} X^i Y^j Z^k \mid p_{i,j,k} \in K \right\}$$

Selbst Polynome in beliebig vielen Variablen $(X_i)_{i \in I}$ sind möglich.

Wir nutzen dann Multiindizes $\nu \in \mathbb{N}^{(I)}$ und Monome $X^\nu = \prod_{i \in I} X_i^{\nu_i}$:

$$K[(X_i)_{i \in I}] = \left\{ \sum_{\nu \in \mathbb{N}^{(I)}} p_\nu X^\nu \mid p_\nu \in K \right\}.$$

😊 Grundlegend ist die eindeutige Darstellung als solch eine Summe. Definition und Konstruktion übertragen sich wörtlich auf diesen Fall. Statt des Modells $K^{(\mathbb{N})}$ betrachtet man entsprechend $K^{(\mathbb{N}^{(I)})}$.

Polynome in mehreren Variablen

Polynome in mehreren Variablen

Polynome in mehreren Variablen

Euklidische Division für Polynome

Aufgabe: Berechnen Sie im Polynomring $\mathbb{Z}[X]$ die euklidische Division von $S = 2X^4 - 5X^3 + 2X^2 - 9X + 8$ durch $P = X^2 - 3X$.

Lösung: Schriftliche Polynomdivision

$$\begin{array}{r}
 2X^4 - 5X^3 + 2X^2 - 9X + 8 = (X^2 - 3X)(2X^2 + X + 5) + 6X + 8 \\
 - 2X^4 + 6X^3 \\
 \hline
 X^3 + 2X^2 \\
 - X^3 + 3X^2 \\
 \hline
 5X^2 - 9X \\
 - 5X^2 + 15X \\
 \hline
 6X + 8
 \end{array}$$

Wir erhalten den Quotienten $Q = 2X^2 + X + 5$ mit Rest $R = 6X + 8$.

Euklidische Division für Polynome

Aus der Grundschule kennen Sie die schriftliche Division von natürlichen Zahlen in Basis $B = 10$. Das Verfahren verläuft genauso, doch durch den Übertrag kommt es vor, dass man die nächste Ziffer überschätzt.

Die Polynomdivision in $K[X]$ ist wesentlich leichter als die Division in \mathbb{N} . Subjektiv mag es Ihnen umgekehrt erscheinen, weil Sie die Division in \mathbb{N} schon seit Ihrer Kindheit kennen, die Polynomdivision erst kürzer. Objektiv gesehen ist die erste schwerer als die zweite.

Übung: Wenn Sie gerne programmieren, dann können Sie beide Divisionen als Übung implementieren: die Division von Polynomen $\sum_i a_i X^i$ und von natürlichen Zahlen $\sum_i a_i B^i$. Sie werden sehen: Polynome sind leichter als Zahlen!

Euklidische Division für Polynome

Hier noch ein berühmtes Beispiel, die sogenannte geometrische Teleskopsumme; für die allgemeinen Formel siehe Satz G2D:

$$\begin{array}{r}
 (X^5 - 1) : (X - 1) = X^4 + X^3 + X^2 + X + 1 \\
 \begin{array}{r}
 X^5 \\
 - X^5 + X^4 \\
 \hline
 X^4 \\
 - X^4 + X^3 \\
 \hline
 X^3 \\
 - X^3 + X^2 \\
 \hline
 X^2 \\
 - X^2 + X \\
 \hline
 X - 1 \\
 - X + 1 \\
 \hline
 0
 \end{array}
 \end{array}$$

Euklidische Division für Polynome

Die Division von Polynomen gelingt über jedem kommutativen Ring K , wir benötigen lediglich, dass der Leitkoeffizient $\text{lc}(P)$ in K invertierbar ist. In den obigen Beispielen war P normiert, also $\text{lc}(P) = 1$.

Euklidische Division für Polynome

Satz G3H: euklidische Division für Polynome

Sei $P \in K[X]$ ein Polynom mit invertierbarem Leitkoeffizient $\text{lc } P \in K^\times$.
Zu jedem $S \in K[X]$ existiert genau ein Paar $Q, R \in K[X]$, für das gilt

$$S = PQ + R \quad \text{und} \quad \deg R < \deg P.$$

Wir nennen $S \text{ quo } P := Q$ den **Quotienten** und $S \text{ rem } P := R$ den **Rest** der euklidischen Division von S durch P . Dies definiert die Operationen

$$(\text{quo}, \text{rem}) : K[X] \times K[X]_n^1 \rightarrow K[X] \times K[X]_{<n} : (S, P) \mapsto (Q, R).$$

Eindeutigkeit: Angenommen die Polynome $Q, Q', R, R' \in K[X]$ erfüllen $S = PQ + R = PQ' + R'$ und $\deg R, \deg R' < \deg P$.

Dann gilt $P(Q - Q') = R' - R$. Dank $\text{lc } P \in K^\times$ und Satz G3B folgt:

$$\deg P + \deg(Q - Q') = \deg(R' - R) < \deg P.$$

Daraus folgt $\deg(Q - Q') < 0$, also $Q - Q' = 0$, und somit $R' - R = 0$.

Euklidische Division für Polynome

Die **Existenz** von (Q, R) beweisen wir durch Konstruktion wie folgt:

Algo G3H: Division mit Rest von zwei Polynomen

Eingabe: $S, P \in K[X]$ mit $\text{lc } P \in K^\times$

Ausgabe: $Q, R \in K[X]$ mit $S = PQ + R$ und $\deg R < \deg P$

```

1:  $Q \leftarrow 0; R \leftarrow S$  // Invariante  $S = PQ + R$ 
2: while  $\deg R \geq \deg P$  do // Solange noch etwas zu tun ist
3:    $T \leftarrow \text{lc}(P)^{-1} \text{lc}(R) \cdot X^{\deg R - \deg P}$  //  $\deg(PT) = \deg R, \text{lc}(PT) = \text{lc } R$ 
4:    $R \leftarrow R - PT; Q \leftarrow Q + T$  // Invariante  $S = PQ + R$ 
5: return  $(Q, R)$  //  $S = PQ + R$  und  $\deg R < \deg P$ 

```

Beweis: Dieser Algorithmus ist korrekt, erfüllt also seine Spezifikation:

- 1 Der Algorithmus terminiert, denn $\deg R$ sinkt in jeder Iteration.
- 2 Die Rückgabe (Q, R) erfüllt $S = PQ + R$ und $\deg R < \deg P$.

Aufgabe: Führen Sie die Argumente sorgfältig aus.

Wenn Sie den Algorithmus auf das obige Beispiel an.

Euklidische Division für Polynome

Lösung: (1) Der Term T ist so gewählt, dass R und PT gleichen Grad und gleichen Leitkoeffizienten haben. Also gilt $\deg(R - PT) < \deg R$. Der Algorithmus endet nach höchstens $1 + \deg S - \deg P$ Iterationen.

(2) Die Initialisierung $Q \leftarrow 0$, $R \leftarrow S$ garantiert, dass $S = PQ + R$. Jede Iteration $R \leftarrow R - PT$, $Q \leftarrow Q + T$ erhält diese Gleichung. Zum Schluss gilt also $S = PQ + R$ mit $\deg R < \deg P$, wie gewünscht.

Aufgabe: Formulieren Sie alternativ einen Induktionsbeweis über $\deg S$. Beide sind logisch äquivalent; die induktive Form ist in der Mathematik geläufiger, die iterative Form in der Informatik. Das ist sehr praktisch!

Lösung: Für $\deg S < \deg P$ genügt $(Q, R) = (0, S)$. Sei $\deg S \geq \deg P$ und die Aussage gelte für alle Polynome $\tilde{S} \in K[X]$ mit $\deg \tilde{S} < \deg S$. Wir setzen $T = \text{lc}(P)^{-1} \text{lc}(S) \cdot X^{\deg S - \deg P} \in K[X]$ und $\tilde{S} = S - PT$. Damit gilt $\deg(PT) = \deg S$ und $\text{lc}(PT) = \text{lc} S$, also $\deg \tilde{S} < \deg S$. Nach Induktionsvoraussetzung gibt es $\tilde{Q}, R \in R[X]$ mit $\tilde{S} = P\tilde{Q} + R$ und $\deg R < \deg P$. Daher gilt $S = \tilde{S} + PT = P\tilde{Q} + R + PT$ für $Q = \tilde{Q} + T$.

Euklidische Division für Polynome

Bemerkung: Für jedes Polynom P mit Grad $\deg P = n \in \mathbb{N}$ und invertierbarem Leitkoeffizienten $\text{lc } P \in K^\times$ erhalten wir eine Bijektion

$$K[X] \times K[X]_{<n} \xrightarrow{\sim} K[X] : (Q, R) \mapsto S = PQ + R.$$

Die Voraussetzung $\text{lc } P \in K^\times$ ist hierbei wesentlich. Gegenbeispiel: Im Ring $K = \mathbb{Z}$ der ganzen Zahlen ist 2 nicht invertierbar, die Abbildung $\mathbb{Z}[X] \times \mathbb{Z}[X]_{<0} \rightarrow \mathbb{Z}[X] : (Q, 0) \mapsto 2Q + 0$ ist injektiv, aber nicht bijektiv.

Nullstellen von Polynomen

Sei K ein kommutativer Ring und $P \in K[X]$ ein Polynom über K .

Vorgelegt sei ein Element $a \in K$. Gilt $P(a) = 0$, so nennen wir a eine **Nullstelle** des Polynoms P , oder eine **Wurzel** der Gleichung $P(X) = 0$.

Lemma G3I: Nullstelle als Linearfaktor abspalten

Genau dann gilt $P(a) = 0$, wenn die Faktorisierung $P = (X - a)Q$ für ein $Q \in K[X]$ gilt. In diesem Fall ist Q eindeutig bestimmt.

Beweis: Die Implikation „ \Leftarrow “ ist klar, wir zeigen nur noch „ \Rightarrow “:

Dank Polynomdivision G3H existiert genau ein Paar $Q, R \in K[X]$ mit $P = (X - a)Q + R$ und $\deg R < \deg(X - a) = 1$, also $R \in K$.

Demnach verschwindet $P(a) = R$ genau dann, wenn $R = 0$ gilt.

Dies ist gleichbedeutend mit $P = (X - a)Q$.

QED

Nullstellen von Polynomen

Nullstellen von Polynomen

Weiterhin sei K ein kommutativer Ring.

Satz G3J: Nullstellen und Vielfachheiten

(1) Zu $P \in K[X]^*$ und $a \in K$ gibt es genau ein Paar (m, Q) mit $m \in \mathbb{N}$ und $Q \in K[X]$, so dass $P = (X - a)^m Q$ und $Q(a) \neq 0$ gilt.

Im Falle $m \geq 1$ nennen wir a eine Nullstelle von P der **Vielfachheit** m , bei $m = 1$ eine **einfache**, bei $m \geq 2$ eine **mehrfache Nullstelle**.

(2) Jedes Polynom $P \in K[X]^*$ schreibt sich als Produkt

$$P = (X - a_1)^{m_1} \cdots (X - a_k)^{m_k} Q$$

mit paarweise verschiedenen $a_1, \dots, a_k \in K$ und ihren Vielfachheiten $m_1, \dots, m_k \in \mathbb{N}_{\geq 1}$, sodass $Q \in K[X]^*$ keine Nullstellen in K hat.

Beweis: Induktion über $\deg P$.

QED

Nullstellen von Polynomen

Anzahl der Nullstellen eines Polynoms

Jedes Polynom $P \in K[X]^*$ schreibt sich wie oben erklärt als Produkt

$$P = (X - a_1)^{m_1} \cdots (X - a_k)^{m_k} Q.$$

Somit hat P *mindestens* die Nullstellen $a_1, \dots, a_k \in K$.

⚠ Im Allgemeinen ist diese Zerlegung nicht eindeutig!

⚠ Es kann noch weitere Nullstellen geben!

Beispiel: Über dem Ring $K = \mathbb{Z}/8$ erlaubt das Polynom $P = X^2 - \bar{1}$ vier verschiedene Nullstellen, nämlich $\pm\bar{1}$ und $\pm\bar{3}$. Hier gilt

$$P = (X - \bar{1})(X + \bar{1}) = (X - \bar{3})(X + \bar{3}).$$

Beispiel: Im Matrixring $\mathbb{C}^{2 \times 2}$ hat das Polynom $P = X^2 + 1 \in \mathbb{R}[X]$ unendlich viele Nullstellen! Ausführliche Konstruktion: Die Matrix

$$M = \begin{pmatrix} ix & -y - iz \\ y - iz & -ix \end{pmatrix}$$

mit $x, y, z \in \mathbb{R}$ erfüllt $M^2 = -1$ genau dann, wenn $x^2 + y^2 + z^2 = 1$ gilt.

Anzahl der Nullstellen eines Polynoms

Optimistisch würde man vermuten, dass ein Polynom $P \in K[X]$ vom Grad n höchstens n Nullstellen haben kann. Das ist im Allgemeinen jedoch falsch! Um Sie vor naivem Irrglauben zu bewahren, nenne ich hier eindrückliche Gegenbeispiele.

Im zweiten Beispiel ist die Nicht-Kommutativität Ursache des Problems. Die hier angegebenen Matrizen sind übrigens genau die Quaternionen $q = xI + yJ + zK \in H < \mathbb{C}^{2 \times 2}$ mit Norm $|q| = 1$, siehe Beispiel B1G. Selbst in Schiefkörpern schlägt die naive Vermutung also fehl!

Im ersten Beispiel sind offensichtlich die Nullteiler das Problem. Für Körper und Integritätsringe sieht es besser aus!

Anzahl der Nullstellen eines Polynoms

Satz G3K: eindeutige Faktorisierung der Nullstellen

Sei $(K, +, 0, \cdot, 1)$ ein Integritätsring: $1 \neq 0$, kommutativ, nullteilerfrei.

(1) Jedes Polynom $P \in K[X]^*$ faktorisiert als ein Produkt

$$P = (X - a_1)^{m_1} \cdots (X - a_k)^{m_k} Q$$

mit paarweise verschiedenen $a_1, \dots, a_k \in K$ und ihren Vielfachheiten $m_1, \dots, m_k \in \mathbb{N}_{\geq 1}$, sodass $Q \in K[X]^*$ keine Nullstellen in K hat.

(2) In diesem Falle sind a_1, \dots, a_k die einzigen Nullstellen von P . Die Faktorisierung ist eindeutig bis auf Umordnung der Faktoren.

(3) Ein Polynom $P \in K[X]$ vom Grad $n \in \mathbb{N}$ hat höchstens n Nullstellen in K (mit Vielfachheiten gezählt, das bedeutet $m_1 + \cdots + m_k \leq n$).

(4) Je zwei Polynome $P, Q \in K[X]_{\leq n}$ sind bereits dann gleich, wenn sie an $n + 1$ Stellen $x_0, x_1, \dots, x_n \in K$ übereinstimmen.

Anzahl der Nullstellen eines Polynoms

Beweis: (2) Wir vergleichen zwei solche Zerlegungen

$$P = (X - a_1)^{m_1} \cdots (X - a_k)^{m_k} Q = (X - b_1)^{n_1} \cdots (X - b_\ell)^{n_\ell} R.$$

Wir zeigen $k = \ell$ sowie nach Umordnung $a_1 = b_1, \dots, a_k = b_k$ und $m_1 = n_1, \dots, m_k = n_k$. Wir führen Induktion über k . Für $k = 0$ hat $P = Q$ keine Nullstellen in K , daher gilt auch $\ell = 0$ und $P = R$.

Sei $k \geq 1$. Aus $P(a_k) = 0$ und der Nullteilerfreiheit von K folgt, dass einer der Faktoren $(a_k - b_1), \dots, (a_k - b_\ell)$ gleich 0 sein muss. Durch Umordnung erreichen wir $a_k = b_\ell$. Dank G3J folgt $m_k = n_\ell$ und $(X - a_1)^{m_1} \cdots (X - a_{k-1})^{m_{k-1}} Q = (X - b_1)^{n_1} \cdots (X - b_{\ell-1})^{n_{\ell-1}} R$. Nach Induktionsannahme folgt dann $k - 1 = \ell - 1$ und $a_1 = b_1, \dots, a_{k-1} = b_{k-1}$ und $m_1 = n_1, \dots, m_{k-1} = n_{k-1}$.

(3) Das folgt aus (2) und (1) dank Additivität des Grades (G3B).

(4) Auch $P - Q$ ist vom Grad $\leq n$, hat aber $n + 1$ Nullstellen. Dank (3) gilt $P - Q = 0$, also $P = Q$.

◻

Satz G3L: Auswertung und Interpolation

Sei $(K, +, \cdot)$ ein Körper und $x_0, x_1, \dots, x_n \in K$ paarweise verschieden. Zu beliebigen Werten $y_0, y_1, \dots, y_n \in K$ existiert genau ein Polynom $P \in K[X]_{\leq n}$ mit $P(x_0) = y_0, P(x_1) = y_1, \dots, P(x_n) = y_n$. Wir haben

$$K[X]_{\leq n} \xrightarrow{\sim} K^{n+1} : P \mapsto (P(x_0), P(x_1), \dots, P(x_n))$$

sowie den surjektiven Ringhomomorphismus

$$\varphi : K[X] \rightarrow K^{n+1} : P \mapsto (P(x_0), P(x_1), \dots, P(x_n))$$

mit $\ker \varphi = (X - x_0)(X - x_1) \cdots (X - x_n)K[X]$ dank Satz G3k.

Existenz: Eine mögliche Lösung ist die Lagrange-Interpolation

$$L(X) := \sum_{j=0}^n y_j L_j(X) \in K[X]_{\leq n} \quad \text{mit} \quad L_j(X) := \prod_{i \neq j} \frac{X - x_i}{x_j - x_i} \in K[X]_n.$$

Eindeutigkeit folgt aus Satz G3k(4).

Auswertung und Interpolation

Vorgegeben seien $n + 1$ verschiedene Stützstellen $x_0, x_1, \dots, x_n \in \mathbb{K}$.
Für alle $i \neq j$ ist demnach $x_j - x_i \neq 0$ im Körper K invertierbar.
Zu jedem $j = 0, 1, \dots, n$ definieren wir das **Lagrange–Polynom**

$$L_j(X) := \prod_{i \neq j} \frac{X - x_i}{x_j - x_i} \in \mathbb{K}[X]_n$$

Dieses Polynom erfüllt $L_j(x_j) = 1$ und $L_j(x_i) = 0$ für alle $i \neq j$.
Zu den Werten $y_0, y_1, \dots, y_n \in \mathbb{K}$ betrachten wir die Linearkombination

$$L(X) := \sum_{j=0}^n y_j L_j(X) \in \mathbb{K}[X]_{\leq n}.$$

Diese erfüllt $L(x_j) = y_j$ für alle $j = 0, 1, \dots, n$, wie gewünscht.



Dies konstruiert *eine* Lösung. Es könnte noch *weitere* geben!



Die Eindeutigkeit haben wir in Kapitel B mit dem Gauß–Algorithmus gezeigt (siehe Seite B309 zur Vandermonde–Matrix). Hier nun gelingt uns ein zweiter, unabhängiger Beweis dank euklidischer Division.

Satz G3M: Polynom vs Polynomfunktion

Sei K ein Körper. Jedes Polynom $P = \sum_{i=0}^n p_i X^i \in K[X]$ definiert die zugehörige Polynomfunktion $f_P : K \rightarrow K : a \mapsto P(a) = \sum_{i=0}^n p_i a^i$.

Dies stiftet den Ringhomomorphismus $f : K[X] \rightarrow K^K : P \mapsto f_P$.

- 1 Ist K unendlich, dann ist f injektiv, aber nicht surjektiv.
- 2 Ist K endlich, dann ist f surjektiv, aber nicht injektiv.

Beweis: (1a) Je zwei Polynome $P, Q \in K[X]_{\leq n}$ sind gleich, wenn sie an $n + 1$ Stellen $x_0, x_1, \dots, x_n \in K$ übereinstimmen.

Aus der Gleichheit $f_P = f_Q$ folgt demnach die Gleichheit $P = Q$.

(1b) Die Funktion $\delta_0 : K \rightarrow K$ mit $\delta_0(0) = 1$ und $\delta_0(x) = 0$ für $x \neq 0$ ist keine Polynomfunktion. Wäre $\delta_0 = f_P$ für ein $P \in K[X]_{\leq n}$, so folgt $f_P(x) = f_0(x)$ für alle $x \in K^*$, also $P = 0$. Es gilt jedoch $\delta_0 \neq f_0$.

(2a) Die Lagrange-Interpolation G3L garantiert die Surjektivität.

(2b) Dank G3K gilt $\ker(f) = F \cdot K[X]$ mit $F = \prod_{a \in K} (X - a)$. ◻

Polynom vs Polynomfunktion

Wir haben anfangs gesehen, dass wir das Polynom $P \in K[X]$ und seine Polynomfunktion $f_P: K \rightarrow K: a \mapsto P(a)$ unterscheiden müssen:

Das Polynom P bestimmt die zugehörige Funktion f_P , aber umgekehrt können wir im Allgemeinen aus f_P nicht eindeutig P rekonstruieren.

Der obige Satz G3M klärt die Beziehung $f: K[X] \rightarrow K^K: P \mapsto f_P$ nun abschließend und umfassend auf:

- 1 Für jeden unendlichen Körper K besteht dieses Problem nicht, hier können wir Polynome und Polynomfunktionen identifizieren.
- 2 Für jeden endlichen Körper ist die Zuordnung f nicht injektiv, aber wir können immerhin ihren Kern präzise angeben.

😊 Speziell für den Körper $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ bestimmt der folgende Satz G3N das Polynom $F = \prod_{a \in \mathbb{F}_p} (X - a) = X^p - X$. Das ist explizit und elegant!

Der kleine Satz von Fermat

Satz G3N: der kleine Satz von Fermat

- (1) Sei K ein Korper der Charakteristik $p > 0$ und $f: K \rightarrow K: a \mapsto a^p$ der Frobenius-Endomorphismus. Dann gilt $\text{fix}(f) = \text{Char}(K) \cong \mathbb{Z}/p\mathbb{Z}$.
- (2) Uber $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ gilt somit die Zerlegung $X^p - X = \prod_{a \in \mathbb{F}_p} (X - a)$.
- (3) Fur jede ganze Zahl $a \in \mathbb{Z}$ gilt $a^p \equiv a \pmod{p}$, also $a^p - a \in p\mathbb{Z}$.
- (4) Fur jede ganze Zahl $a \in \mathbb{Z} \setminus p\mathbb{Z}$ gilt $a^{p-1} \equiv 1 \pmod{p}$.

Beweis: (1a) Wir zeigen „ $\text{fix}(f) \supseteq \text{Char}(K)$ “. Es gilt $f(0_K) = 0_K$ und $f(1_K) = 1_K$. Per Induktion gilt $f(1_K \cdot n) = 1_K \cdot n$ fur alle $n \in \mathbb{N}$, denn

$$\begin{aligned} f(1_K \cdot (n+1)) &\stackrel{\text{Def}}{=} f(1_K \cdot n + 1_K) \stackrel{\text{Add}}{=} f(1_K \cdot n) + f(1_K) \\ &\stackrel{\text{Fix}}{=} 1_K \cdot n + 1_K \stackrel{\text{Def}}{=} 1_K \cdot (n+1). \end{aligned}$$

(1b) Wir zeigen die Umkehrung „ $\text{fix}(f) \subseteq \text{Char}(K)$ “. Jeder Fixpunkt von f ist eine Nullstelle des Polynoms $F = X^p - X$. Dieses hat hochstens p Nullstellen in K , und dank (1a) gilt $F(a) = 0$ fur alle $a \in \text{Char}(K)$.

Die weiteren Aussagen (2–4) sind damit klar.

◻

Der kleine Satz von Fermat

Übung: Sei $p \geq 2$ eine Primzahl und $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$.

- 1 Zu jeder beliebigen Abbildung $g: \mathbb{F}_p \rightarrow \mathbb{F}_p$ existiert genau ein Polynom $P \in \mathbb{F}_p[X]_{<p}$ mit $g = f_P$, also $g(a) = P(a)$ für alle $a \in \mathbb{F}_p$.
- 2 Für je zwei Polynome $P, Q \in \mathbb{F}_p[X]$ gilt $f_P = f_Q$ genau dann, wenn $P - Q \in (X^p - X)\mathbb{F}_p[X]$ gilt.

Beispiel: Für $P = X^2 - X \in \mathbb{F}_2[X]$ gilt $P(0) = P(1) = 0$, also $f_P = 0$.
Für $P = X^p - X \in \mathbb{F}_p[X]$ und alle $a \in \mathbb{F}_p$ gilt $P(a) = 0$, also $f_P = 0$.

Beispiel: Spezialfall $p = 2$: Für alle $a \in \mathbb{Z}$ gilt $a^2 \equiv a \pmod{2}$.
Das können Sie auch ganz elementar beweisen, siehe C215.

Bemerkung: Ist $p \geq 3$ prim, so gilt $a^{p-1} - 1 \equiv 0$ modulo p . Dies ist ein erster Primzahltest für p , wenn auch noch recht grob. Etwas genauer gilt

$$\left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) \equiv 0, \text{ also } a^{\frac{p-1}{2}} \equiv \pm 1.$$

Eine weitere Verfeinerung führt zum extrem effizienten Primzahltest von Miller–Rabin, siehe de.wikipedia.org/wiki/Miller-Rabin-Test.

Fundamentalsatz der Algebra, komplex und reell

Zur Abrundung betrachten wir komplexe und reelle Polynome:

Satz G30: Fundamentalsatz der Algebra

(1) Zu jedem komplexen Polynom $P = X^n + c_1X^{n-1} + \dots + c_n \in \mathbb{C}[X]$ existieren komplexe Nullstellen $z_1, z_2, \dots, z_n \in \mathbb{C}$, sodass

$$P = (X - z_1)(X - z_2) \cdots (X - z_n).$$

(2) Fur jedes reelle Polynom $P = X^n + c_1X^{n-1} + \dots + c_n \in \mathbb{R}[X]$ folgt

$$P = (X - a_1) \cdots (X - a_k)(X^2 - 2u_1X + w_1) \cdots (X^2 - 2u_\ell X + w_\ell)$$

mit $n = k + 2\ell$ und $a_i, u_j, w_j \in \mathbb{R}$ sowie der Diskriminante $u_j^2 - w_j < 0$.

Fundamentalsatz der Algebra, komplex und reell

Den Fundamentalsatz (1) kann ich Ihnen hier leider nicht beweisen. Aber Sie konnen immerhin die Aquivalenz „(1) \Leftrightarrow (2)“ erklaren:

Ubung: „(1) \Rightarrow (2)“: Zu $P \in \mathbb{R}[X] \subset \mathbb{C}[X]$ existieren dank (1) komplexe Nullstellen $z_1, \dots, z_n \in \mathbb{C}$, sodass $P = (X - z_1) \cdots (X - z_n)$ gilt.

Wegen $P \in \mathbb{R}[X]$ gilt $P(\bar{z}_j) = \overline{P(z_j)} = \bar{0} = 0$. Nicht-reelle Nullstellen treten also immer als konjugierte Paare $u \pm iv \in \mathbb{C} \setminus \mathbb{R}$ auf. Dabei gilt:

$$(X - (u + iv))(X - (u - iv)) = X^2 - 2uX + u^2 + v^2 \in \mathbb{R}[X].$$

Zusammenfassung konjugierter Paare ergibt die reelle Darstellung (2).

Ubung: Die umgekehrte Implikation „(2) \Rightarrow (1)“ folgt aus der Mitternachtsformel zur Losung quadratischer Gleichungen und der Existenz von Quadratwurzeln in \mathbb{C} (siehe Polarkoordinaten A305).

Wir erkennen eine verblüffende, wichtige Gemeinsamkeit des Rings \mathbb{Z} der ganzen Zahlen und des Polynomrings $K[X]$ über einem Körper K :

- 1 Beide sind Integritätsringe mit euklidischer Division (A2A, G3H).
- 2 Darauf beruht der Algorithmus von Eulid (A2H) und Bézout (A2I).
- 3 Daraus folgt das Lemma von Euklid (A2M): unzerlegbar vs prim.
- 4 Wir erhalten die eindeutige Zerlegung in Primfaktoren (A2J).

Aufgabe: Wiederholen Sie die genannten Ergebniss für den Ring \mathbb{Z} . Formulieren und beweisen Sie alles entsprechend für den Ring $K[X]$ und allgemein für jeden euklidischen Ring im Sinne von Punkt (1).

Arithmetik in \mathbb{Z} und in $K[X]$

Definition G3P: assoziierte Elemente

Im Folgenden sei $(R, +, 0, \cdot, 1)$ ein Integritätsring. Dann ist $R^* = R \setminus \{0\}$ ein Untermonoid von $(R, \cdot, 1)$, da aus $a \neq 0$ und $b \neq 0$ stets $ab \neq 0$ folgt. In $(R, \cdot, 1)$ bezeichnet R^\times die Untergruppe der invertierbaren Elemente.

(1) Zwei Elemente $a, b \in R$ unseres Rings heißen **assoziiert** in R , wenn es ein invertierbares Element $u \in R^\times$ gibt sodass $au = b$ gilt.

Dies ist eine Äquivalenzrelation, geschrieben $a \sim_R b$ oder kurz $a \sim b$.

Übung: Prüfen Sie nach, dass \sim_R eine Äquivalenzrelation auf R ist.

Beispiele: Genau dann ist R ein Körper, wenn $R^\times = R^*$ gilt.

Für jedes Ringelement $a \in R$ gilt dann entweder $a = 0$ oder $a \sim 1$.

In \mathbb{Z} gilt $\mathbb{Z}^\times = \{-1, +1\} \subsetneq \mathbb{Z}^*$. Assoziiert $a \sim b$ bedeutet hier $a = \pm b$.

In jeder Äq'-klasse $\{\pm a\}$ wählen wir $|a|$ als kanonischen Repräsentanten.


In $K[X]$ gilt $K[X]^\times = K^\times$. Assoziiert $P \sim Q$ heißt $P = uQ$ mit $u \in K^\times$.

In jeder Äq'-klasse $K^\times Q$ wählen wir den Repräsentanten P mit $\text{lc } P = 1$.

Teilbarkeit in einem Integritätsring

Definition G3P: Teilbarkeit

(2) Seien $a, b \in R$. Wir sagen a **teilt** b , oder b ist ein **Vielfaches** von a , falls es $a' \in R$ gibt mit $aa' = b$. Dies schreiben wir $a \mid_R b$ oder kurz $a \mid b$. Andernfalls sagen wir a teilt nicht b , geschrieben $a \nmid_R b$ oder kurz $a \nmid b$.

Beispiel: Für jedes Element $a \in R$ gilt $1 \mid a$, und $a \mid 1$ gdw $a \in R^\times$. Ebenso gilt $a \mid 0$, und $a \mid 0$ gdw $a = 0$.  Es gilt $0 \mid 0$, also „0 teilt 0“. Weiterhin können wir nicht durch 0 teilen, denn $0/0$ hat keinen Sinn!

Aufgabe: (a) Teilbarkeit ist eine Präordnung (im Sinne von F1A). Kleinste Elemente sind 1 und alle $u \in K^\times$, das größte Element ist 0.
(b) Aus gegenseitiger Teilbarkeit $a \mid b$ und $b \mid a$ folgt Assoziertheit $a \sim b$.

Lösung: (a) Es gilt Reflexivität $a \mid a$, dank $a \cdot 1 = a$, und Transitivität: Aus $a \mid b$ und $b \mid c$ folgt $a \mid c$, denn $aa' = b$ und $bb' = c$ impliziert $aa'b' = c$.
(b) Gilt $aa' = b$ und $bb' = a$, so folgt $aa'b' = a$. Im Integritätsring R können wir $a \neq 0$ kürzen und erhalten $a'b' = 1$, also $a', b' \in R^\times$. Im Sonderfall $a = 0$ gilt $b = 0$, also ebenfalls $a \sim b$.

Größte gemeinsame Teiler

Definition G3P: größte gemeinsame Teiler

(3) Die Menge der **gemeinsamen Teiler** von $a_1, \dots, a_n \in R$ ist

$$\text{GT} = \text{GT}_R(a_1, \dots, a_n) := \{ t \in R \mid t \mid_R a_1, \dots, t \mid_R a_n \}.$$

Die Menge der **größten gemeinsamen Teiler** definieren wir durch

$$\text{GGT} = \text{GGT}_R(a_1, \dots, a_n) := \{ t \in \text{GT} \mid \forall s \in \text{GT} : s \mid_R t \}.$$

Hier verstehen wir „größer“ im Sinne der Präordnung \mid_R auf R . (F1H)

Übung: Alle Elemente der Menge GGT sind zueinander assoziiert: Für jeden Repräsentanten $t \in \text{GGT}$ gilt demnach $\text{GGT} = K^\times t$.

Konvention: Wir betrachten insbesondere die Ringe \mathbb{Z} und $K[X]$.

Ist t unser kanonischer Repräsentant, so schreiben wir kurz $\text{ggT} := t$.

Beispiel: In \mathbb{Z} gilt $\text{GT}(45, 60) = \{\pm 1, \pm 3, \pm 5, \pm 15\}$ und $\text{GGT} = \{\pm 15\}$. Wir nennen $\text{ggT}(45, 60) = +15$ kurz *den* größten gemeinsamen Teiler.

 Ohne diese Normierung nennen wir $t \in \text{GGT}$ vorsichtig *einen* ggT.

Kleinste gemeinsame Vielfache

Definition G3P: kleinste gemeinsame Vielfache

(4) Die Menge der **gemeinsamen Vielfachen** von $a_1, \dots, a_n \in R$ ist

$$GV = GV_R(a_1, \dots, a_n) := \{ v \in R \mid a_1 \mid_R v, \dots, a_n \mid_R v \}.$$

Die Menge der **kleinsten gemeinsamen Vielfachen** ist

$$KGV = KGV(a_1, \dots, a_n) := \{ v \in GV \mid \forall u \in GV : v \mid_R u \}.$$

Hier verstehen wir „kleiner“ im Sinne der Präordnung \mid_R auf R . (F1H)

Übung: Alle Elemente der Menge KGV sind zueinander assoziiert:
Für jeden Repräsentanten $v \in KGV$ gilt demnach $KGV = K^\times v$.

Konvention: Wir betrachten insbesondere die Ringe \mathbb{Z} und $K[X]$.
Ist v unser kanonischer Repräsentant, so schreiben wir kurz $\text{kgV} := v$.

Beispiel: In \mathbb{Z} gilt $GV(45, 60) = \{\pm 180, \pm 360, \dots\}$ und $KGV = \{\pm 180\}$.
Wir nennen $\text{kgV}(45, 60) = +180$ *das* kleinste gemeinsame Vielfache.

 Ohne diese Normierung nennen wir $v \in KGV$ vorsichtig *ein* kgV.

Teilbarkeit, ggT und kgV

Aufgabe: Zeigen Sie die folgenden Eigenschaften und Rechenregeln:

- (0) Die Präordnung $|$ auf R ist im Allgemeinen nur partiell, nicht total.
- (1) Immer ist 0 das kleinste Element und 1 ein größtes Element.

Teilbarkeit ist verträglich mit Addition und Multiplikation:

- (2) Aus $a | b$ und $a | c$ folgt $a | b + c$, allgemein $a | bu + cv$ für alle $u, v \in R$.
- (3) Aus $a | b$ und $c | d$ folgt $ac | bd$, insbesondere dank $c | c$ auch $ac | bc$.
- (4) Kürzungsregel: Für $c \neq 0$ sind $ac | bc$ und $a | b$ äquivalent.

Vorsicht bei gemeinsamen Teilern und Vielfachen in exotischen Ringen:

- (5) Untersuchen Sie X^a, X^{a+1} im Polynomring $R = \mathbb{Q}[X]$ und im Teilring $S = \mathbb{Q}[X^2, X^3] = \{p_0 + p_2X^2 + \dots + p_nX^n \mid n \in \mathbb{N}, p_0, p_2, \dots, p_n \in \mathbb{Q}\}$.
- (6) Die Mengen $\text{GGT}(a, b)$ und $\text{KGV}(a, b)$ können leer sein.
- (7) Sei t ein ggT von a und b . Ist dann $v = ab/t$ ein kgV von a und b ?
- (8) Sei v ein kgV von a und b . Ist dann $t = ab/v$ ein ggT von a und b ?

Teilbarkeit, ggT und kgV

😊 Für knifflige Fragen wie (6–8) benötigen Sie gute Beispiele wie (5).

Lösung: (5) In R gilt $\text{GT}_R(X^a, X^{a+1}) = \{ uX^i \mid u \in \mathbb{Q}^\times, 0 \leq i \leq a \}$, also $\text{ggT}_R(X^a, X^{a+1}) = X^a$. Das war auch zu erwarten. Ebenso gilt $\text{GV}_R(X^a, X^{a+1}) = \mathbb{Q}[X] \cdot X^{a+1}$, also $\text{kgV}_R(X^a, X^{a+1}) = X^{a+1}$.

In S hingegen gilt $\text{GT}_S(X^a, X^{a+1}) = \{ u, uX^i \mid u \in \mathbb{Q}^\times, 2 \leq i \leq a-2 \}$. Für $a = 0, 1, 2, 3$ gilt $\text{ggT}_S(X^a, X^{a+1}) = 1$, dann $\text{ggT}_S(X^4, X^5) = X^2$ und $\text{GGT}_S(X^5, X^6) = \emptyset$, denn $X^2 \nmid_S X^3$. Das ist überaus merkwürdig!

Andererseits gilt $\text{GV}_S(X^a, X^{a+1}) = \mathbb{Q}[X] \cdot X^{a+3}$. Erneut folgt daraus $\text{KGV}_S(X^a, X^{a+1}) = \emptyset$, denn $X^{a+3} \nmid_S X^{a+4}$. Auch das ist merkwürdig!

(6) Für X^5, X^6 in $S = \mathbb{Q}[X^2, X^3]$ gilt $\text{GGT} = \emptyset$ und $\text{KGV} = \emptyset$ dank (5).

(7) Nein! Für X^2, X^3 in $S = \mathbb{Q}[X^2, X^3]$ gilt $\text{GGT} = \mathbb{Q}^\times$ und $\text{KGV} = \emptyset$.

(8) Ja, falls $v \neq 0$. Es gilt $t \mid a$ und $t \mid b$, denn $a = \frac{ab}{v} \cdot \frac{v}{b}$ und $b = \frac{ab}{v} \cdot \frac{v}{a}$. Angenommen ein weiteres Element $s \in R$ erfüllt ebenso $s \mid a$ und $s \mid b$. Dann folgt $a \mid ab/s$ und $b \mid ab/s$, also $v \mid ab/s$, somit $sv \mid ab$ und $s \mid ab/v$. Das zeigt $s \mid t$, also ist t tatsächlich ein ggT von a und b in R .

Unzerlegbar / irreduzibel vs prim

Wir zerlegen das Monoid $R^* = R^\times \sqcup R^{\text{red}} \sqcup R^{\text{irr}}$ in die invertierbaren R^\times , zerlegbaren / reduziblen R^{red} und unzerlegbaren / irreduziblen R^{irr} :

$$R^\times := \{ a \in R^* \mid \exists b \in R^* : ab = 1 \},$$

$$R^{\text{red}} := \{ a \in R^* \mid \exists b, c \in R^* \setminus R^\times : a = bc \},$$

$$R^{\text{irr}} := \{ a \in R^* \mid \forall b, c \in R^* : a = bc \Rightarrow b \sim 1 \vee c \sim 1 \}$$

Definition G3P: unzerlegbar / irreduzibel vs prim

(5a) Ein Element $a \in R^*$ heißt **unzerlegbar** / irreduzibel in R , falls gilt:
Für alle $b, c \in R$ folgt aus $a = b \cdot c$ entweder $b \in R^\times$ oder $c \in R^\times$.

(5b) Hingegen nennen wir ein Element $a \in R \setminus R^\times$ **prim** in R , falls gilt:
Für je zwei Faktoren $b, c \in R$ folgt aus $a \mid b \cdot c$ stets $a \mid b$ oder $a \mid c$.

Beispiel: Das Nullelement ist besonders, $R = \{0\} \sqcup R^\times \sqcup R^{\text{red}} \sqcup R^{\text{irr}}$.


Es ist zudem prim, denn $0 \mid ab$ bedeutet $ab = 0$, also $a = 0$ oder $b = 0$.

Im Monoid $(\mathbb{Z}^*, \cdot, 1)$ sind ± 1 invertierbar, $\pm 2, \pm 3, \pm 5, \pm 7, \pm 11, \pm 13, \dots$ unzerlegbar und $\pm 4, \pm 6, \pm 8, \pm 9, \pm 10, \pm 12, \pm 14, \pm 15, \pm 16, \dots$ zerlegbar.

Unzerlegbar / irreduzibel vs prim

Bemerkung: Im Monoid $(\mathbb{Z}^{\cdot, \cdot}, 1)$ sind unzerlegbar und prim äquivalent dank dem Lemma von Euklid (A2M). Das gilt nicht in jedem Ring:

Beispiel: Im Ring $S = \mathbb{Q}[X^2, X^3] = \{p_0 + p_2X^2 + \dots + p_nX^n \mid p_i \in \mathbb{Q}\}$ sind X^2 und X^3 unzerlegbar, aber nicht prim: Es gilt $X^2 \mid X^3 \cdot X^3$, aber $X^2 \nmid X^3$. Ebenso gilt $X^3 \mid X^2 \cdot X^4$, aber weder $X^3 \mid X^2$ noch $X^3 \mid X^4$.

 Das Element $X^6 = X^3 \cdot X^3 \cdot X^3 = X^2 \cdot X^2$ hat in $S = \mathbb{Q}[X^2, X^3]$ zwei völlig verschiedene Zerlegungen in unzerlegbare Elemente. Für „vernünftige“ Ringe wollen wir solche Pathologien ausschließen!

Lemma G3Q: Prim impliziert unzerlegbar.

Sei R ein Ring. Jedes Primelement $p \in R^*$ ist unzerlegbar in R .

Aufgabe: Beweisen Sie dies nach dem Vorbild von Lemma A2M(1).

Lösung: Sei $p \neq 0$ prim und $p = ab$ in R . Daraus folgt $p \mid a$ oder $p \mid b$. Nehmen wir $p \mid a$ an, also $a = pp'$ für ein $p' \in \mathbb{Z}$. Damit gilt $p = ab = pp'b$, nach Kürzung $1 = p'b$, also $b = \pm 1$. Analog folgt aus $p \mid b$, dass $a = \pm 1$.

Zerlegung in irreduzible Faktoren

Definition G3P: Zerlegung in unzerlegbare Faktoren

(6a) Zu $a \in R^*$ besteht eine **irreduzible Zerlegung** kurz **UProdukt**

$(u; p_1, \dots, p_n)$ aus $u \in R^\times$ und $p_1, \dots, p_n \in R^{\text{irr}}$ mit $a = up_1 \cdots p_n$.

(6b) Zwei irreduzible Zerlegung $(u; p_1, \dots, p_n)$ und $(v; q_1, \dots, q_m)$ heißen **assoziiert**, wenn $m = n$ und nach Umordnung $p_1 \sim q_1, \dots, p_n \sim q_n$ gilt.

(7a) Ein Element $a \in R^*$ ist **zerlegbar in unzerlegbare Faktoren** in R , falls ein solches UProdukt existiert. (Für $n = 0$ gilt $a = u$, also $a \in R^\times$.)

(7b) Wir nennen a in R **eindeutig zerlegbar in irreduzible Faktoren**, wenn zudem je zwei irreduzible Zerlegungen von a assoziiert sind.

(8) Ein Integritätsring R heißt **faktoriell** wenn jedes Element $a \in R^*$ eindeutig in irreduzible Faktoren zerlegbar ist wie in (7) erklärt.

(9) Wir nennen $\mathbb{P} \subset R^{\text{irr}}$ ein **Repräsentantensystem** der unzerlegbaren Elemente in R , falls jedes unzerlegbare Element $q \in R^{\text{irr}}$ assoziiert ist zu genau einem Element $p \in \mathbb{P}$, als **kanonischem Repräsentanten**.

Zerlegung in irreduzible Faktoren

Dank Kommutativität können wir Produkte in R beliebig umordnen.

Ebenso können wir von jeder irreduziblen Zerlegung $a = up_1 \cdots p_n$ übergehen zu $a = (uu_1^{-1} \cdots u_n^{-1})(u_1p_1) \cdots (u_n p_n)$ mit $u_1, \dots, u_n \in R^\times$.

Diese offensichtliche Umformung können und wollen wir nicht verbieten. Wir nennen die Zerlegung von a eindeutig, wenn je zwei Zerlegungen allein durch diese offensichtlichen Umformungen ineinander übergehen.

Beispiel: Der Fundamentalsatz der Arithmetik (A2J) besagt: Der Ring \mathbb{Z} der ganzen Zahlen ist faktoriell. Jede ganze Zahl lässt sich zerlegen in irreduzible Faktoren, eindeutig bis auf Reihenfolge und Vorzeichen.

$$-60 = (-1) \cdot 2 \cdot 2 \cdot 3 \cdot 5 = (+1) \cdot (-5) \cdot 2 \cdot (-3) \cdot (-2)$$

Beispiel: Der Ring $\mathbb{Q}[X^2, X^3]$ ist nicht faktoriell, denn für Elemente wie $X^6 = X^3 \cdot X^3 \cdot X^3 = X^2 \cdot X^2$ gibt es mehr als eine Zerlegung.

Übung: Genau dann ist R faktoriell, wenn jedes Element $a \in R$ eine irreduzible Zerlegung erlaubt und jedes irreduzible Element prim ist.

Faktorisierung als Isomorphismus

Beispiel: Im Ring \mathbb{Z} wählen wir als kanonische Repräsentanten traditionell die positiven Primzahlen, $\mathbb{P} = \mathbb{Z}_{>0}^{\text{irr}} = \{2, 3, 5, 7, 11, 13, \dots\}$.

Satz G3R: Faktorisierung als Isomorphismus

Sei R ein Ring und $\mathbb{P} \subset R$ eine Teilmenge. Dann sind äquivalent:

(1) Der Ring R ist faktoriell, erlaubt also eindeutige UProdukte, und $\mathbb{P} \subset R$ ist ein Repräsentantensystem der unzerlegbaren Elemente.

$$\Phi = \Phi_R^{\mathbb{P}} : (R^{\times}, \cdot) \times (\mathbb{N}^{(\mathbb{P})}, +) \rightarrow (R^*, \cdot) : (u, \nu) \mapsto u \cdot \prod_{p \in \mathbb{P}} p^{\nu(p)}$$

(2) Der Monoidhomomorphismus Φ ist bijektiv, also ein Isomorphismus.

Als Dreingabe erhalten wir dank \mathbb{P} in R kanonische ggT und kgV:

$$\text{ggT}(a, b) = \prod_p p^{\min(\nu_a(p), \nu_b(p))} \quad \text{und} \quad \text{kgV}(a, b) = \prod_p p^{\max(\nu_a(p), \nu_b(p))}$$

Insbesondere folgt die schöne Beziehung $\text{ggT}(a, b) \cdot \text{kgV}(a, b) \sim a \cdot b$.

Faktorisierung als Isomorphismus

Aufgabe: Beweisen Sie die Äquivalenz des Satzes G3R.

Lösung: „(1) \Rightarrow (2)“: Die Abbildung Φ ist ein Monoidhomomorphismus. Surjektivität bedeutet, jedes Element $a \in R^*$ lässt sich als UProdukt schreiben; Injektivität bedeutet, je zwei UProdukte zu a sind assoziiert.

„(2) \Rightarrow (1)“: Wir vergleichen $a = u \prod_p p^{\nu_a(p)}$ und $b = v \prod_p p^{\nu_b(p)}$ in R . Dann ist Teilbarkeit $a \mid b$ in R äquivalent zur Relation $\nu_a \leq \nu_b$ in $\mathbb{N}^{(\mathbb{P})}$. Somit ist \mathbb{P} ein Repräsentantensystem der unzerlegbaren Elemente in R , und der Ring R ist faktoriell, da in R eindeutige UProdukte existieren.

😊 Der Isomorphismus Φ_R klärt die Struktur des Monoids (R^*, \cdot) .

⚠ Das Produkt $\Phi_{\mathbb{Z}}$ ist leicht, die Primfaktorzerlegung $\Phi_{\mathbb{Z}}^{-1}$ ist notorisch schwer zu berechnen. Genau darauf beruhen Cryptosysteme wie RSA.

😊 Glücklicherweise gibt es für ggT und kgV in euklidischen Ringen weit effizientere Algorithmen, und diesen wenden wir uns nun zu.

Eindeutigkeit der Zerlegung

Lemma G3s: Eindeutigkeit der Zerlegung

Sei R ein Integritätsring und jedes unzerlegbare Element sei prim. Dann sind zu jedem Element $a \in R^*$ je zwei UProdukte assoziiert.

Aufgabe: Beweisen Sie dies nach dem Vorbild \mathbb{Z} (Satz A2J).

Lösung: In R betrachten wir zwei UProdukte

$$a = up_1p_2 \cdots p_n = vq_1q_2 \cdots q_m.$$

Wir behaupten, dass $n = m$ gilt und nach Umordnung $p_i \sim q_i$ für alle i . Wir führen Induktion über n . Für $n = 0$ gilt $a \in R^\times$, also auch $m = 0$. Für $n \geq 1$ ist p_n unzerlegbar, nach Voraussetzung somit auch prim. Also gilt $p_n \mid q_i$ für ein $i \in \{1, \dots, m\}$. Nach Umordnung gilt $i = m$. Da auch q_m unzerlegbar ist, folgt $p_n \sim q_m$. Kürzen ergibt

$$a/p_n = up_1p_2 \cdots p_{n-1} = v'q_1q_2 \cdots q_{m-1}.$$

Nach Induktionsvoraussetzung gilt für diese gekürzten Produkte $n - 1 = m - 1$ und nach Umordnung $p_i \sim q_i$ für alle $i = 1, \dots, n - 1$.

Existenz und Eindeutigkeit der Zerlegung

😊 Dieses schöne Argument ist der übliche Weg, um die Eindeutigkeit der Primfaktorzerlegung in R zu beweisen. Die wesentliche Zutat ist: Jedes unzerlegbare Element ist prim. Zum Verständnis des Rings R wollen wir daher das genaue Verhältnis von unzerlegbaren und primen Elementen untersuchen. Unser Ziel ist das Lemma von Euklid (G3x).

Für den Ring \mathbb{Z} kennen wir den Fundamentalsatz der Arithmetik A2J: Jede ganze Zahl $a \in \mathbb{Z}^*$ ist ein Produkt von Primzahlen, und diese Zerlegung ist eindeutig bis auf Reihenfolge und Vorzeichen.

Dies wollen wir nun ebenfalls für jeden Polynomring $K[X]$ über einem Körper K beweisen: Jedes Polynom $a \in K[X]^*$ ist ein Produkt von unzerlegbaren Polynomen in $K[X]$, und diese Zerlegung ist eindeutig bis auf Reihenfolge und Assoziiertheit der Faktoren.

Die gute Nachricht: Der Beweis verläuft genau so, wie Sie dies im Vorbild \mathbb{Z} gesehen haben. Wir nutzen die Gelegenheit, diese schönen Argumente noch einmal genau nachzuvollziehen, und die wesentlichen Ideen als allgemeine Definitionen und Sätze zu formulieren.

Euklidische Ringe: Division mit Rest

Definition G3T: euklidischer Ring

Sei R ein Integritätsring. Eine **euklidische Division** auf dem Ring R ist ein Paar (ν, δ) aus einer Funktion $\nu: R \rightarrow \mathbb{N}$ mit $\nu(0) = 0 = \min \mathbb{N}$ und einer Abbildung $\delta: R \times R^* \rightarrow R \times R: (a, b) \mapsto (q, r)$, so dass gilt:

$$a = bq + r \quad \text{und} \quad \nu(r) < \nu(b).$$

Statt (\mathbb{N}, \leq) genügt eine beliebige wohlgeordnete Menge (N, \leq) .

Wir nennen das Tripel (R, ν, δ) dann einen **euklidischen Ring** mit **(euklidischer) Division** δ und **(euklidischer) Normfunktion** ν .

Wir definieren $\text{quo}, \text{rem}: R \times R^* \rightarrow R$ durch $\delta(a, b) = (a \text{ quo } b, a \text{ rem } b)$ und nennen dies **Quotient** und **Rest** der Division von a durch b .

Beispiele: Der Ring \mathbb{Z} ist euklidisch mit der Norm $\nu: \mathbb{Z} \rightarrow \mathbb{N}: b = |b|$ und der Division mit Rest $\delta: \mathbb{Z} \times \mathbb{Z}^* \rightarrow \mathbb{Z} \times \mathbb{N}$ aus Satz A2A.

Über jedem Körper K ist der Polynomring $K[X]$ euklidisch mit der Norm $\text{deg}: K[X] \rightarrow \mathbb{N} \cup \{-\infty\}$ und der Division δ aus Satz G3H.

Euklidische Ringe: Division mit Rest

Wir dividieren $a \in R$ durch $b \in R^*$ und erhalten gemäß $a = bq + r$ einen Quotienten $q \in R$ und einen Rest $r \in R$. Dabei müssen wir sicherstellen, dass der Rest r „kleiner“ als b ist. Dies messen wir mit der Norm ν .

Abkürzend nennen wir einen Integritätsring R **euklidisch**, wenn auf R eine euklidische Division (ν, δ) wie in G3T existiert.

Manche Autoren nennen das Paar (R, ν) einen **euklidischen Ring** und fordern dann, dass dazu eine geeignete Division δ existiert.

Ist R euklidisch, so gibt es im Allgemeinen mehrere Normfunktionen ν und zu jeder Normfunktion ν auch mehrere euklidische Divisionen δ .

Zur Formulierung von Algorithmen nutzen wir sowohl die Norm ν als auch die Division δ , daher betrachten wir explizit das Tripel (R, ν, δ) .

Nicht jeder Ring ist euklidisch, zum Beispiel ist der Polynomring $\mathbb{Z}[X]$ nicht euklidisch. (Später genauer: $\mathbb{Z}[X]$ ist kein Hauptidealring.)

Euklidische Ringe: Division mit Rest

Bemerkung: (1) Statt (\mathbb{N}, \leq) genügt jede wohlgeordnete Menge (N, \leq) .

Für Polynome etwa nutzen wir die Norm $\deg: K[X] \rightarrow \mathbb{N} \cup \{-\infty\}$.

Genau so gut können wir $\nu: K[X] \rightarrow \mathbb{N}$ betrachten mit $\nu(0) = 0$ und $\nu(P) = 1 + \deg(P)$ für $P \neq 0$. Das Ergebnis ist dasselbe.

(2) In Definition G3T fordern wir zunächst $\nu(0) = 0 = \min \mathbb{N}$.

Wir folgern nun, dass für $b \in R^*$ stets $\nu(b) > 0$ gilt: Jede Division $\delta: (a, b) \mapsto (q, r)$, etwa für $a = 0$, ergibt $\nu(r) < \nu(b)$, also gilt $\nu(b) > 0$.

(3) In \mathbb{Z} und $K[X]$ gilt die schöne Eigenschaft: Aus $a \mid b$ folgt $a \operatorname{rem} b = 0$.

Es schadet nichts, dies sogar für jeden euklidischen Ring zu fordern, wir können δ notfalls immer so anpassen, und (R, ν, δ) bleibt euklidisch.

Wir haben in G3T zunächst nur die minimalen Forderungen formuliert.

Man kann weitere gute Eigenschaften fordern oder herleiten.

Eine ausführliche Diskussion verschieben wir auf später.

Euklidische Ringe: Division mit Rest

Wozu führen wir den abstrakten Begriff eines „euklidischen Rings“ ein?

Zunächst wollen wir die beiden Beispiele \mathbb{Z} und $K[X]$ zusammenfassen, wesentliche Gemeinsamkeiten benennen und einheitlich behandeln.

Das ist in der Mathematik ein allgegenwärtiger Trick zur Denkökonomie, zudem wird dadurch die Struktur noch wesentlich klarer und einfacher.

Es gibt darüber hinaus noch viele weitere euklidische Ringe. Auf diese wollen wir hier noch nicht eingehen, aber wir können alles vorbereiten.

So sind Sie für die Zukunft bestens gewappnet: Wann immer Ihnen ein euklidischer Ring begegnet, haben Sie sofort passende Werkzeuge.

Ist Abstraktion etwas Gutes? Ich denke schon! Sie klärt und vereinfacht, sie bündelt viele Beispiele und verhilft uns zu wesentlich mehr Effizienz. Und sie schadet nicht: Wenn Sie möchten, können Sie bei „euklidischer Ring“ immer an die beiden wichtigsten Beispiele denken: \mathbb{Z} und $K[X]$.

😊 Wir formulieren und beweisen im Allgemeinen, wir illustrieren und rechnen im Konkreten. Beides ergänzt sich wie linke und rechte Hand.

Der euklidische Algorithmus

☺ Der von den ganzen Zahlen \mathbb{Z} bekannte euklidische Algorithmus überträgt sich wörtlich auf $K[X]$ und jeden euklidischen Ring (R, ν, δ) :

Algo G3U: euklidischer Algorithmus

Eingabe: zwei Elemente $a_0, b_0 \in R$ in einem euklidischen Ring (R, ν, δ)

Ausgabe: ein größter gemeinsame Teiler $a \in \text{GGT}(a_0, b_0)$ im Ring R

-
- | | |
|--|---|
| 1: $\begin{bmatrix} a \\ b \end{bmatrix} \leftarrow \begin{bmatrix} a_0 \\ b_0 \end{bmatrix}$ | // $\text{GT}(a, b) = \text{GT}(a_0, b_0)$ |
| 2: while $b \neq 0$ do $\begin{bmatrix} a \\ b \end{bmatrix} \leftarrow \begin{bmatrix} a \\ a \text{ rem } b \end{bmatrix}$ | // $\text{GT}(a, b) = \text{GT}(b, a - qb)$ |
| 3: wähle $\varepsilon \in R^\times$, notfalls $\varepsilon = 1$ | // optional zur Normierung |
| 4: return εa | // $\text{GGT}(a, 0) = R^\times a$ |

Satz G3U: ggT in einem euklidischen Ring

Sei (R, ν, δ) ein euklidischer Ring, etwa \mathbb{Z} oder $K[X]$.

- (1) Zu je zwei Elementen $a, b \in R$ existiert ein ggT in R .
- (2) Der obige Algorithmus berechnet einen solchen ggT.

Der euklidische Algorithmus

Wir müssen zeigen, dass der angegebene Algorithmus korrekt ist, also dass die Methode tatsächlich liefert, was die Spezifikation verspricht.

Die Methode terminiert: Die Norm $\nu(b) \in \mathbb{N}$ nimmt in jedem Schritt ab, bis mit $\nu(b) = 0$ schließlich $b = 0$ erreicht ist und der Algorithmus endet.

Das gelieferte Ergebnis erfüllt die geforderten Bedingungen:

Die Initialisierung $(a, b) \leftarrow (a_0, b_0)$ garantiert $\text{GT}(a, b) = \text{GT}(a_0, b_0)$. Jede Iteration erhält $\text{GT}(a, b) = \text{GT}(b, a - qb)$. Zum Schluss gilt also $\text{GT}(a_0, b_0) = \text{GT}(a, 0)$, somit $\text{GGT}(a_0, b_0) = \text{GGT}(a, 0) = R^\times a$. QED

😊 Das ist genial-einfach und einfach-genial. Zudem ist die Methode sehr effizient, das heißt, auch für große Eingaben (a_0, b_0) geeignet.

😊 Wir können das Ergebnis zu „dem“ kanonischen ggT normieren:

Beispiele: In \mathbb{Z} wählen wir $a \geq 0$. In $K[X]$ wählen wir a mit $\text{lc}(a) = 1$.

😊 Auch der erweiterte Algorithmus A2I zur Berechnung eines ggT mit Bézout-Koeffizienten überträgt sich von \mathbb{Z} auf $K[X]$ und (R, ν, δ) .

Übung: Wiederholen Sie A2I und formulieren Sie dies nun allgemein.

Der erweiterte euklidische Algorithmus nach Bézout

Algo G3v: euklidischer Algorithmus mit Bézout-Koeffizienten

Eingabe: zwei Elemente $a_0, b_0 \in R$ in einem euklidischen Ring (R, ν, δ)

Ausgabe: drei Elemente $a, u, v \in R$ mit $a = a_0u + b_0v \in \text{GGT}(a_0, b_0)$

- | | |
|--|--|
| 1: $\begin{bmatrix} a & u & v \\ b & s & t \end{bmatrix} \leftarrow \begin{bmatrix} a_0 & 1 & 0 \\ b_0 & 0 & 1 \end{bmatrix}$ | // Invariante $\begin{cases} a = a_0u + b_0v \\ b = a_0s + b_0t \end{cases}$ |
| 2: while $b \neq 0$ do $q \leftarrow a \text{ quo } b$ | // euklidische Division |
| 3: $\begin{bmatrix} a & u & v \\ b & s & t \end{bmatrix} \leftarrow \begin{bmatrix} b & s & t \\ a - qb & u - qs & v - qt \end{bmatrix}$ | // Invariante $\begin{cases} a = a_0u + b_0v \\ b = a_0s + b_0t \end{cases}$ |
| 4: wähle $\varepsilon \in R^\times$, notfalls $\varepsilon = 1$ | // optional zur Normierung |
| 5: return $(\varepsilon a, \varepsilon u, \varepsilon v)$ | // $a = a_0u + b_0v \in \text{GGT}(a_0, b_0)$ |

Satz G3v: ggT mit Bézout-Koeffizienten

- Sei (R, ν, δ) ein euklidischer Ring. (1) Zu je zwei Elementen $a, b \in R$ existieren **Bézout-Koeffizienten** $u, v \in R$ mit $d = au + bv \in \text{GGT}(a, b)$. (2) Obiger Algorithmus berechnet einen ggT mit Bézout-Koeffizienten. (3) Das ist ein Zertifikat: Aus $t = au + bv \in \text{GT}(a, b)$ folgt $t \in \text{GGT}(a, b)$.

Der erweiterte euklidische Algorithmus nach Bézout

Bemerkung: Die Operationen $q \leftarrow a \text{ quo } b$ und

$$\begin{bmatrix} a & u & v \\ b & s & t \end{bmatrix} \leftarrow \begin{bmatrix} b & s & t \\ a - qb & u - qs & v - qt \end{bmatrix}$$

erinnern uns an Zeilenoperationen für lineare Gleichungssysteme, hier die invarianten Gleichungen. $R_1 \leftrightarrow R_2$: Wir tauschen die beiden Zeilen. $R_2 \leftarrow R_2 - qR_1$: Von der zweiten Zeile ziehen wir q mal die erste ab. Die Gleichungen $a = a_0u + b_0v$ und $b = a_0s + b_0t$ bleiben erhalten.

Beweis: (2) In der ersten Spalte wird der euklidische Algorithmus G3U zur Berechnung des ggT ausgeführt. Die Invarianten garantieren in jedem Schritt die Gleichungen $a = a_0u + b_0v$ und $b = a_0s + b_0t$.

(3) Sei $d = au + bv$ sowie $d \mid a$ und $d \mid b$. Wir zeigen $d \in \text{GGT}(a, b)$: Angenommen $c \mid a$ und $c \mid b$, also $ca' = a$ und $cb' = b$. Dann gilt $c(a'u + b'v) = d$, also $c \mid d$. Das heißt, d ist ein ggT von a und b . □

Die Primfaktorzerlegung im Polynomring $K[X]$

Für den Ring \mathbb{Z} gilt der Fundamentalsatz der Arithmetik (A2J). Dieser Satz gilt genauso für jeden Polynomring $K[X]$ über einem Körper K :

Satz G3W: Primfaktorzerlegung im Polynomring $K[X]$

Sei K ein Körper. Dann ist der Polynomring $K[X]$ faktoriell.

Explizit ausformuliert bedeutet das folgendes:

(1) Jedes Polynom $a \in K[X]^*$ können wir zerlegen in ein Produkt

$$a = u \cdot p_1 \cdot p_2 \cdot \dots \cdot p_\ell$$

mit $u = \text{lc}(a) \in K^\times$ und $p_1, p_2, \dots, p_\ell \in K[X]$ unzerlegbar und normiert.

(2) Diese Zerlegung ist eindeutig bis auf Umordnung: Gilt

$$p_1 \cdot p_2 \cdot \dots \cdot p_\ell = q_1 \cdot q_2 \cdot \dots \cdot q_k$$

mit unzerlegbaren normierten Polynomen p_1, p_2, \dots, p_ℓ und q_1, q_2, \dots, q_k , so folgt $\ell = k$ und nach Umordnung $p_1 = q_1, p_2 = q_2, \dots, p_\ell = q_\ell$.

Die Primfaktorzerlegung im Polynomring $K[X]$

Sei $\mathbb{P} \subset K[X]$ die Teilmenge der unzerlegbaren normierten Polynome. Gemäß Satz G3R haben wir den Monoidhomomorphismus

$$\begin{aligned} \Phi = \Phi_{K[X]} : (K^\times, \cdot) \times (\mathbb{N}^{(\mathbb{P})}, +) &\rightarrow (K[X]^*, \cdot) : (u, \nu) \mapsto u \cdot \prod_{p \in \mathbb{P}} p^{\nu(p)}, \\ (\mathbb{N}^{(\mathbb{P})}, +) &\rightarrow (K[X]^1, \cdot). \end{aligned}$$

Dank Satz G3W ist Φ bijektiv, also ein Isomorphismus. Das beinhaltet zwei Aussagen: (1) Surjektivität bedeutet, jedes Polynom $a \in K[X]^*$ lässt sich als ein Produkt unzerlegbarer Polynome in $K[X]$ schreiben. Diese können wir normieren zu $a = up_1 \cdots p_\ell$ mit $u = \text{lc}(a) \in K^\times$ und $p_1, \dots, p_\ell \in \mathbb{P}$. (2) Injektivität bedeutet, je zwei solche Zerlegungen zu a sind assoziiert.

😊 Für den Polynomring $K[X]$ können wir dies nun leicht beweisen, da wir alle Werkzeuge zur Hand haben. Der Beweis verläuft genau so, wie Sie dies im Vorbild \mathbb{Z} gesehen haben. Diese Wiederholung ist eine wunderbare Gelegenheit, das Verständnis zu festigen und zu vertiefen.

Existenz einer Primfaktorzerlegung in $K[X]$

Aufgabe: Beweisen Sie die Existenz (1) nach dem Vorbild \mathbb{Z} (A2J).

😊 Die Existenz ist ein recht naheliegendes Induktionsargument:
Wir zerlegen bis es aus Gradgründen nicht weiter geht. Ausführlich:

Lösung: Wir führen Induktion über den Polynomgrad $n = \deg(a)$.
Für $n = 0$ gilt $a = u \in K^\times$; dies ist eine Zerlegung der Länge $\ell = 0$.

Sei nun $n \geq 1$. Entweder a ist unzerlegbar oder echt zerlegbar.

Ist a unzerlegbar, so gilt $a = up_1$ mit $u = \text{lc}(a)$ und $p_1 = a/u \in \mathbb{P}$.

Ist a in $K[X]^*$ echt zerlegbar, so gilt $a = bc$ mit $a, b \in K[X]^* \setminus K^\times$.

Für die Polynomgrade bedeutet dies $\deg(b) \geq 1$ und $\deg(c) \geq 1$.

Wegen $n = \deg(a) = \deg(b) + \deg(c)$ folgt $\deg(b) < n$ und $\deg(c) < n$.

Nach Induktionsvoraussetzung existieren Zerlegungen $b = up_1 \cdots p_k$
und $c = vp_{k+1} \cdots p_\ell$. Somit ist $a = (uv)p_1 \cdots p_\ell$ eine Zerlegung von a .

Übung: Übertragen Sie Euklids Lemma (A2M) von \mathbb{Z} auf $K[X]$.
Folgern Sie daraus die Eindeutigkeit der Primfaktorzerlegung (G3s).

😊 Damit ist Satz G3w zur Primfaktorzerlegung in $K[X]$ bewiesen!

Eindeutigkeit der Primfaktorzerlegung in $K[X]$

Weiterhin sei K ein Körper und $K[X]$ der Polynomring über K .

Lemma G3X: Lemma von Euklid für $K[X]$

Jedes unzerlegbare Element $p \in K[X]^*$ ist prim in $K[X]$.

Beweis: Sei $p \in K[X]^*$ ein unzerlegbares Polynom in $K[X]$. Gegeben seien zwei Polynome $a, b \in K[X]$ mit $p \mid ab$. Wir zeigen $p \mid a$ oder $p \mid b$:
 Hierzu sei $d = \text{ggT}(p, a)$. Es gilt $d \mid p$; da p unzerlegbar ist, gilt entweder $d = 1$ oder $d \sim p$.
 (a) Im Falle $d \sim p$ gilt dank $d \mid a$ sofort $p \mid a$.
 (b) Im Falle $d = 1$ folgt $p \mid b$ mit dem Lemma von Gauß. □

Lemma G3Y: Lemma von Gauß für $K[X]$

Seien $p, a, b \in K[X]$ mit $\text{ggT}(p, a) = 1$. Dann folgt aus $p \mid ab$ bereits $p \mid b$.

Beweis: Dank Bézout G3v existieren $u, v \in K[X]$, sodass $pu + av = 1$. Die Teilbarkeit $p \mid ab$ bedeutet $ab = pq$ für ein $q \in K[X]$. Daraus folgt
 $b = (pu + av)b = pub + avb = p(ub + qv)$, also $p \mid b$. □

