

## Kapitel E

## Kombinatorik und Quotienten

*Wer hohe Türme bauen will,  
muss lange beim Fundament verweilen.*

Anton Bruckner (1824–1896)

## Inhalt dieses Kapitels E

- 1 Endliche Mengen und Elementezahl
  - Permutationen und Zykelzerlegung
  - Der Zählssatz: Wie messen wir Mengen?
  - Invariansatz und Dirichlets Schubfachprinzip
- 2 Kombinatorische Abzählformeln
  - Grundrechenarten für endliche Mengen
  - Teilmengen und Binomialkoeffizienten
  - Zerlegungen und Stirling–Zahlen
- 3 Zerlegungen, Äquivalenzrelationen und Quotienten
  - Zerlegung und Quotient, die Klassengleichung
  - Äquivalenzrelationen und Faktorisierung
  - Konstruktion der rationalen Zahlen  $\mathbb{Q}$
  - Konstruktion des Restklassenrings  $\mathbb{Z}/n\mathbb{Z}$

## Kombinatorik und Quotienten

E003  
Überblick

Im vorigen Kapitel D haben wir die Grundlagen erarbeitet für Mengen und Abbildungen, speziell Injektionen, Surjektionen und Bijektionen. Dies wollen wir nun für endliche Mengen  $X, Y, \dots$  konkretisieren. Hier gelten besonders starke und nützliche Gesetzmäßigkeiten.

Für Selbstabbildungen  $f: X \rightarrow X$  führen wir die Listennotation ein. Selbstbijektionen  $\sigma: X \xrightarrow{\sim} X$  heißen Permutationen, und hierfür haben wir die sehr effiziente Zykelschreibweise. Permutationen sind überall nützlich, und die konzise Notation hilft in all unseren Rechnungen.

Wir untersuchen damit Abbildungen  $f: \{1, \dots, n\} \rightarrow \{1, \dots, m\}$ . Wir sortieren zur Stufenform (E1E) analog zum Gauß–Algorithmus für Matrizen (B2C). Damit klären wir die Frage der Sur/In/Bijektivität von  $f$  durch drei einfache Kennzahlen:  $n, m$  und  $r = \# \text{im}(f)$ , siehe Satz E1F.

Dieses sorgfältige Vorgehen mag zunächst pedantisch erscheinen, doch der kleinschrittige und umsichtige Aufbau ist eine gute Übung, um mit Sur/In/Bijektionen vertraut zu werden. Als Lohn erhalten wir die Invarianz der Elementezahl E1H und Dirichlets Schubfachprinzip E1I.

## Kombinatorik und Quotienten

E004  
Überblick

Der zweite Teil dieses Kapitels behandelt klassische Abzählformeln: (disjunkte) Vereinigungen, kartesisches Produkte und Potenzen, Abbildungsmengen und Potenzmengen. Hier betone ich die expliziten Bijektionspaare: Dies sind schöne Formeln und konkrete Übungen.

Anschließend behandeln wir Binomialkoeffizienten und Teilmengen sowie Zerlegungen und Stirling–Zahlen. Damit können wir die Anzahl  $\# \text{Inj}(X, Y)$  der Injektionen und  $\# \text{Sur}(Y, X)$  der Surjektionen berechnen (Satz E2L). Auch dies ist mathematisch–didaktisch äußerst lehrreich.

Im dritten Teil kommen wir zu Quotienten und Äquivalenzrelationen. Das gilt gemeinhin als abstrakt und schwierig, doch Quotienten sind nichts anderes als Zerlegungen und somit ganz konkret! Hier zahlt sich unsere sorgsame Vorarbeit aus, sie stiftet konkretes Material zur Anschauung und mildert die begrifflichen Schwierigkeiten.

Wir gehen den langen Weg, doch ich bin überzeugt: Er lohnt sich!

*Je comprends vite quand on me l'explique lentement.*

[Ich verstehe schnell, wenn man es mir langsam erklärt.]

Wir betrachten eine Menge  $X$  und ihre **Selbstabbildungen**:

$$E_X = \text{End}(X) := \text{Abb}(X, X) = \{ f : X \rightarrow X \}$$

Dabei steht  $\text{End}$  für *Endomorphismus*, hier heißt das *Selbstabbildung*. Die Komposition definiert das Monoid  $(E_X, \bullet, \text{id}_X)$  bzw.  $(E_X, \circ, \text{id}_X)$ .

Am einfachsten ist der Fall einer endlichen Menge  $X = \{x_1, x_2, \dots, x_n\}$ :

$$f = \begin{bmatrix} x_1 & x_2 & \dots & x_n \\ y_1 & y_2 & \dots & y_n \end{bmatrix} \quad \text{bedeutet} \quad f : X \rightarrow X : x_k \mapsto y_k.$$

Bei fester Reihenfolge  $(x_1, x_2, \dots, x_n)$  schreiben wir  $f = [y_1, y_2, \dots, y_n]$ . Wenn wir die freie Wahl haben, denken wir speziell an  $X = \{1, 2, \dots, n\}$ .

Die Komposition auf  $E_X$  schreiben wir wahlweise rechts oder links:

$$g_1 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 2 & 3 & 4 \end{bmatrix} \bullet \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 3 & 2 & 4 \end{bmatrix}$$

$$g_2 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 2 & 3 & 4 \end{bmatrix} \circ \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 2 & 4 \end{bmatrix}$$

Wir können jede Abbildung  $f : X \rightarrow X$  als Wertetabelle / Liste angeben:

$$f_1 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 2 & 3 & 4 \end{bmatrix}, \quad f_2 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{bmatrix}$$

**Aufgabe:** Wie erkennt man daran, ob  $f : X \rightarrow X$  eine Bijektion ist?

**Lösung:** In der Zielzeile tritt jedes Element  $x \in X$  genau einmal auf!

**Aufgabe:** Wie bestimmt man im bijektiven Falle die Inverse  $f^{-1}$ ?

**Lösung:** Wir tauschen Startzeile und Zielzeile (und sortieren):

$$f = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{bmatrix} \implies f^{-1} = \begin{bmatrix} 2 & 3 & 1 & 4 \\ 1 & 2 & 3 & 4 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{bmatrix}$$

**Aufgabe:** Ist die Abbildung  $f : \mathbb{Z}_7 \rightarrow \mathbb{Z}_7 : x \mapsto x^5$  eine Permutation?

**Lösung:** Wir rechnen die Wertetabelle sorgsam aus:

$$f = \begin{bmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 0 & 1 & 4 & 5 & 2 & 3 & 6 \end{bmatrix} \implies f^{-1} = \begin{bmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 0 & 1 & 4 & 5 & 2 & 3 & 6 \end{bmatrix}$$

**Definition E1A:** die symmetrische Gruppe  $S_X$

Eine **Permutation** der Menge  $X$  ist eine Selbstbijektion  $\sigma : X \xrightarrow{\sim} X$ . Die Menge aller Permutationen der Menge  $X$  bezeichnen wir mit

$$S_X = \text{Sym}(X) = \text{Aut}(X) := \text{End}(X)^\times = \text{Bij}(X, X) = \{ \sigma : X \xrightarrow{\sim} X \}.$$

Dabei steht  $\text{Aut}$  für *Automorphismus*, hier heißt das *Selbstbijektion*.

Die Komposition definiert die Gruppe  $(S_X, \bullet, \text{id}_X)$  bzw.  $(S_X, \circ, \text{id}_X)$ . Wir nennen dies die **symmetrische Gruppe**  $S_X$  mit Komposition von rechts bzw. links. Speziell für  $X = \{1, 2, \dots, n\}$  schreiben wir kurz  $S_n$ .

Die Komposition auf  $S_X$  schreiben wir wahlweise rechts oder links:

$$\pi_1 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{bmatrix} \bullet \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{bmatrix}$$

$$\pi_2 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{bmatrix} \circ \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{bmatrix}$$

**Aufgabe:** Was verlangen wir von einem Monoid  $(M, \cdot, 1)$ ? Warum ist  $(E_X, \bullet, \text{id}_X)$  ein Monoid? Was sind hierin die invertierbaren Elemente?

Was verlangen wir von einer Gruppe  $(G, \cdot, 1)$ ? Warum bilden die invertierbaren Elemente in  $(M, \cdot, 1)$  eine (Unter)Gruppe? Ganz konkret:

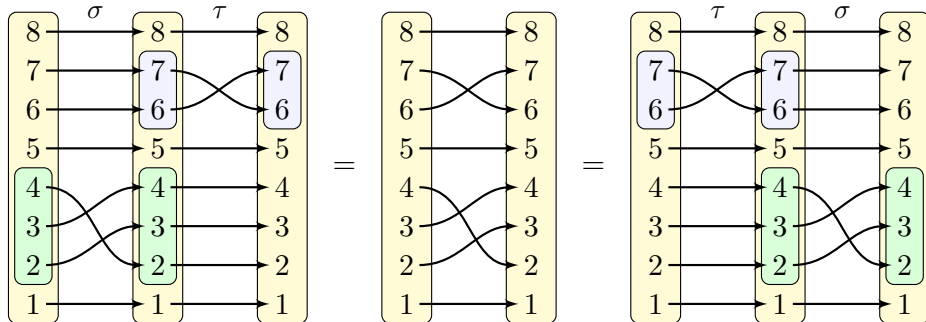
😊 Die Komposition von zwei Bijektionen ist wieder eine Bijektion; die Komposition ist assoziativ,  $\text{id}_X$  ist neutral, die Umkehrfunktion ist invers.

Gegeben sei  $\sigma : X \rightarrow X$ , eine Abbildung der Menge  $X$  in sich selbst. Ein Element  $x \in X$  mit  $\sigma(x) = x$  heißt **Fixpunkt** von  $\sigma$ . Wir setzen  $\text{fix}(\sigma) := \{x \in X \mid \sigma(x) = x\}$  und  $\text{supp}(\sigma) := \{x \in X \mid \sigma(x) \neq x\}$ .

**Lemma E1B:** Disjunkte Permutationen kommutieren.

- (0) Für jede Permutation  $\sigma : X \xrightarrow{\sim} X$  und  $A = \text{supp}(\sigma)$  gilt  $\sigma(A) = A$ .
- (1) Permutationen  $\sigma, \tau : X \xrightarrow{\sim} X$  mit disjunkten Trägern kommutieren.

**Beweis durch Bild:** Es gilt  $\sigma \circ \tau = \tau \circ \sigma$ . Schreiben Sie es aus!



Wir zerlegen  $X = \text{fix}(\sigma) \sqcup \text{supp}(\sigma)$ . Die **Fixpunktmenge**  $\text{fix}(\sigma)$  besteht aus allen Punkten  $x \in X$ , die von  $\sigma$  festgehalten werden. Der **Träger**  $\text{supp}(\sigma)$  besteht aus allen Punkten  $x \in X$ , die von  $\sigma$  bewegt werden.

Eine Verwechslung mit dem Träger einer Funktion  $f : X \rightarrow \{0, 1\}$  ist nicht zu befürchten, siehe D331. Hier geht es um Selbstabbildungen.

Zwei Permutationen  $\sigma, \tau : X \xrightarrow{\sim} X$  derselben Menge  $X$  heißen **disjunkt**, falls ihre Träger disjunkt sind, also  $\text{supp}(\sigma) \cap \text{supp}(\tau) = \emptyset$  erfüllen.

**Beweis des Lemmas:** (0) Für  $x \in \text{supp}(\sigma)$  und  $y = \sigma(x)$  gilt  $x \neq y$ . Wäre  $\sigma(y) = y$ , so hätte  $y$  zwei Urbilder,  $x \neq y$ , im Widerspruch zur Injektivität von  $\sigma$ . Also gilt  $\sigma(y) \neq y$ , somit  $y \in \text{supp}(\sigma)$ , kurz  $\sigma(A) \subseteq A$ . Für die Umkehrung  $\sigma^{-1}$  gilt  $\text{fix}(\sigma^{-1}) = \text{fix}(\sigma)$  und  $\text{supp}(\sigma^{-1}) = \text{supp}(\sigma)$ .

(1) Gegeben seien Permutationen  $\sigma_1, \dots, \sigma_n : X \xrightarrow{\sim} X$  mit paarweise disjunkten Trägern  $A_i = \text{supp}(\sigma_i)$ , also  $A_i \cap A_j = \emptyset$  für alle  $i \neq j$ . Dank (0) ist  $\sigma = \sigma_1 \circ \dots \circ \sigma_n : X \rightarrow X$  gegeben durch  $\sigma(x) = \sigma_i(x)$ , falls  $x \in A_i$  für ein  $i \in I$ , und  $\sigma(x) = x$  sonst, falls  $x \in X \setminus \bigcup_i A_i$ . Das Ergebnis ist also unabhängig von der Reihenfolge! QED

Gegeben seien  $\ell \geq 2$  verschiedene Elemente  $x_1, x_2, \dots, x_\ell \in X$ . Diese definieren eine zyklische Permutation auf  $X$ , kurz  **$\ell$ -Zykel**:

$$\sigma = \text{Cyc}_X(x_1, x_2, \dots, x_\ell) : X \xrightarrow{\sim} X : x_1 \mapsto x_2 \mapsto \dots \mapsto x_\ell \mapsto x_1$$

Ausgeschrieben bedeutet das:  $\sigma(x_1) = x_2, \sigma(x_2) = x_3, \dots, \sigma(x_\ell) = x_1$ . Für alle anderen Elemente  $x \in X \setminus \{x_1, x_2, \dots, x_\ell\}$  setzen wir  $\sigma(x) = x$ . Somit ist  $\text{supp}(\sigma) = \{x_1, x_2, \dots, x_\ell\}$  und  $\text{fix}(\sigma) = X \setminus \{x_1, x_2, \dots, x_\ell\}$ . Damit ist  $\sigma$  eine Permutation auf  $X$ , mit Inverser  $\sigma^{-1} = (x_\ell, \dots, x_2, x_1)$ .

**Beispiele:** Auf der Menge  $X = \{1, 2, 3, 4, 5, 6\}$  haben wir

$$(2, 5, 3) = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 2 & 4 & 3 & 6 \end{bmatrix}, \quad (6, 5, 4, 3) = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 6 & 3 & 4 & 5 \end{bmatrix}.$$

Einfachster Fall: Ein 2-Zykel  $\text{Cyc}_X(a, b) : a \leftrightarrow b$  heißt **Transposition**. Wir vereinbaren zudem  $\text{Cyc}_X(a, a) := \text{id}_X$ , das ist oft bequem.

Sonderfall: Für  $\ell = 1$  ist  $\text{Cyc}_X(a) = \text{id}_X$  die **Identität** auf  $X$ . Dies betrachten wir daher nicht als Zykel.

Die **Listennotation** können wir für jede Abbildung  $f : X \rightarrow Y$  nutzen. Für Permutationen  $f : X \xrightarrow{\sim} X$  haben wir zudem die **Zykelnotation**; diese ist für viele Zwecke und Rechnungen besonders effizient.

Meist lassen wir „Cyc<sub>X</sub>“ weg und schreiben kurz  $\sigma = (x_1, x_2, \dots, x_\ell)$ . Das bezeichnet nicht das  $n$ -Tupel, sondern die Permutation  $\sigma$  auf  $X$ .

Wir können jeden  $\ell$ -Zykel auf genau  $\ell$  verschiedene Weisen schreiben: Diese entstehend durch zyklische Rotation der Punkte. Zum Beispiel sind  $(2, 5, 3) = (5, 3, 2) = (3, 2, 5)$  die drei Schreibweisen dieses Zyklus.

Für beliebige Elemente  $a, b \in X$  definieren wir  $\tau = (a, b) : X \rightarrow X$  durch  $\tau(a) = b$  und  $\tau(b) = a$  sowie  $\tau(x) = x$  für alle  $x \in X \setminus \{a, b\}$ . Im Falle  $a \neq b$  ist dies eine Transposition. Im Falle  $a = b$  ist dies die Identität. Dieser Sonderfall  $\text{Cyc}_X(a, a) = \text{id}_X$  erweist sich später als bequem.

😊 Permutationen haben überall wichtige Anwendungen, sowohl als nützliches Werkzeug als auch als eigener Untersuchungsgegenstand: Algebra (Determinanten, Darstellungen), Informatik (Sortierverfahren, Kryptographie), Physik (Pauli-Prinzip in der Quantenmechanik).

**Beispiel:** Von der Listenschreibweise zur Zykelzerlegung:

$$\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 5 & 9 & 7 & 4 & 6 & 2 & 3 & 8 \end{bmatrix} = (1) (2, 5, 4, 7) (6) (3, 9, 8)$$

Das Inverse ist demnach  $\sigma^{-1} = (8, 9, 3)(7, 4, 5, 2) = (7, 4, 5, 2)(8, 9, 3)$ .  
Dank E1B ist die Potenz  $\sigma^{2020} = (2, 5, 4, 7)^{2020}(3, 9, 8)^{2020} = (3, 9, 8)$ .

### Satz E1C: eindeutige Zykelzerlegung

Sei  $X$  eine endliche Menge. Zu jeder Permutation  $\sigma: X \xrightarrow{\sim} X$  existiert genau eine Menge  $\{c_1, c_2, \dots, c_k\} \subseteq S_X$  disjunkter Zykel  $c_1, c_2, \dots, c_k$ , so dass  $\sigma = c_1 \bullet c_2 \bullet \dots \bullet c_k$  gilt. Die Faktoren kommutieren dank E1B.

**Beispiel:** Komposition nicht-disjunkter Zykel auf  $X = \{1, 2, \dots, 9\}$ :

$$\pi_1 = (2, 3, 4) \bullet (4, 5, 6, 7) = (1) (2, 3, 5, 6, 7, 4) (8) (9)$$

$$\pi_2 = (2, 3, 4) \circ (4, 5, 6, 7) = (1) (2, 3, 4, 5, 6, 7) (8) (9)$$

**Bemerkung:** Jeder  $\ell$ -Zykel ist ein Produkt von  $\ell - 1$  Transpositionen gemäß  $(x_1, x_2, \dots, x_\ell) = (x_1, x_2) \circ (x_2, x_3) \circ \dots \circ (x_{\ell-1}, x_\ell)$ . Dank Satz E1C ist jede Permutation  $\sigma \in S_X$  ein Produkt von Transpositionen.

**Aufgabe:** Denken Sie sich Permutationen aus und zerlegen Sie diese in Zykel. Formulieren Sie einen Algorithmus. Beweisen Sie Satz E1C.

### Algo E1C: Zykelzerlegung

**Eingabe:** eine Permutation  $\sigma: \{1, \dots, n\} \xrightarrow{\sim} \{1, \dots, n\}$

**Ausgabe:** die Zykelzerlegung von  $\sigma$

```

1: visited ← (0, ..., 0) ∈ {0, 1}^n           // alle Punkte noch unbesucht
2: for i from 1 to n do                       // durchlaufe alle Punkte
3:   if visited[i] = 0 then                   // falls neuer Zykel...
4:     j ← i; print("(", j)                  // eröffne den Zykel
5:     repeat                                  // durchlaufe den Zykel...
6:       j ← σ(j); visited[j] ← 1           // nächster Punkt des Zyklus
7:       if j ≠ i then print(" ", j) else print(")")
8:     until j = i                            // schließe den Zykel
```

**Bemerkung:** Im folgenden Beweis benötigen wir die Elementezahl von endlichen Mengen. Wir nutzen diesen Begriff weiterhin zunächst naiv; die folgenden Abschnitte werden diese Technik präzisieren.

**Beweis des Satzes:** Gegeben sei eine endliche Menge  $X$  und eine Permutation  $\sigma \in S_X$ . Wir suchen eine Menge  $C = \{c_1, c_2, \dots, c_k\} \subseteq S_X$  disjunkter Zykel, so dass  $\sigma = \prod C = \prod_{c \in C} c = c_1 \bullet c_2 \bullet \dots \bullet c_k$  gilt.

**Existenz einer Zykelzerlegung:** Wir führen Induktion über die Anzahl  $\#\text{supp}(\sigma)$  der bewegten Punkte. Im Falle  $\#\text{supp}(\sigma) = 0$  gilt  $\sigma = \text{id}$  und  $C = \emptyset$  ist eine Lösung. Wir nehmen nun  $\#\text{supp}(\sigma) \geq 1$  an und wählen  $x \in X$  mit  $\sigma(x) \neq x$ . Die Folge  $x, \sigma(x), \sigma^2(x), \dots$  in  $X$  wiederholt sich irgendwann, da die Menge  $X$  endlich ist. Die erste Wiederholung für ein  $\ell \in \mathbb{N}$  ist von der Form  $\sigma^\ell(x) = x$ , denn andernfalls wäre  $\sigma$  nicht injektiv.

Wir setzen  $c_1 := \text{Cyc}_X(x, \sigma(x), \sigma^2(x), \dots, \sigma^{\ell-1}(x))$  und  $\sigma' := c_1^{-1} \bullet \sigma$ . Der Träger ist demnach  $\text{supp}(c_1) = \{x, \sigma(x), \sigma^2(x), \dots, \sigma^{\ell-1}(x)\} =: I$ . Auf  $I$  gilt  $\sigma' = \text{id}$ , auf  $X \setminus I$  gilt  $\sigma' = \sigma$ . Nach Induktionsvoraussetzung existiert zu  $\sigma'$  eine Zykelzerlegung  $C' = \{c_2, \dots, c_k\}$ . Diese ist disjunkt zu  $c_1$ . Somit ist  $C = \{c_1, c_2, \dots, c_k\}$  eine Zykelzerlegung zu  $\sigma = c_1 \bullet \sigma'$ .

😊 Der obige Algorithmus E1C entrollt diese rekursive Konstruktion in eine Iteration. Dabei wird jeder Punkt nur zweimal durchlaufen. Der Aufwand ist also linear in der Anzahl  $\#X$  der Punkte.

**Eindeutigkeit der Zykelzerlegung:** Zu  $\sigma \in S_X$  seien  $\sigma = b_1 b_2 \dots b_j$  und  $\sigma = c_1 c_2 \dots c_k$  zwei Zerlegungen in disjunkte Zykel vorgelegt. Wir haben  $\{b_1, b_2, \dots, b_j\} = \{c_1, c_2, \dots, c_k\}$  zu zeigen.

Wir können  $k \leq j$  annehmen. Wir führen Induktion über  $k$ .

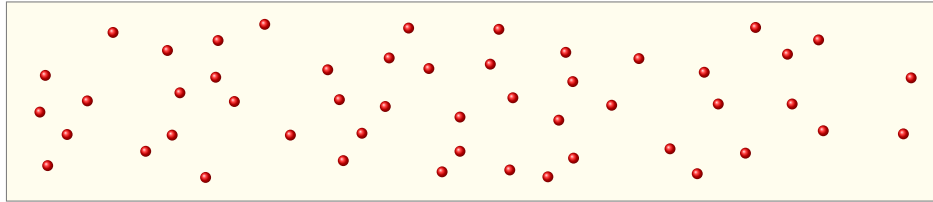
Für  $k = 0$  gilt  $\sigma = \text{id}_X$ , also auch  $j = 0$ , und die Aussage ist klar.

Sei nun  $k \geq 1$  und  $x \in \text{supp}(c_1)$ . Hierzu existiert  $b_\nu$  mit  $x \in \text{supp}(b_\nu)$ . Nach Umordnung können wir  $\nu = 1$  annehmen. Da  $b_1$  und  $c_1$  von den anderen Zykeln disjunkt sind, gilt  $\sigma^n(x) = b_1^n(x) = c_1^n(x)$  für alle  $n \in \mathbb{Z}$ , und somit die Gleichheit  $b_1 = c_1$  dieser beiden Zykel. Für  $\sigma' := c_1^{-1} \bullet \sigma$  haben wir die beiden Zykelzerlegungen  $\sigma' = b_2 \dots b_j$  und  $\sigma' = c_2 \dots c_k$ . Nach Induktionsvoraussetzung gilt  $\{b_2, \dots, b_j\} = \{c_2, \dots, c_k\}$ . Daraus folgt  $\{b_1, b_2, \dots, b_j\} = \{c_1, c_2, \dots, c_k\}$ , wie behauptet. ◻

## Wie viele Elemente hat die vorgelegte Menge?

E113

Wie viele Punkte sehen Sie hier? mindestens? genau?



### Definition E1D: die Anzahl der Elemente einer Menge

Sei  $n \in \mathbb{N}$ . Eine Menge  $X$  **besitzt mindestens  $n$  Elemente**, geschrieben  $\#X \geq n$ , falls eine Injektion  $\nu: \{1, \dots, n\} \hookrightarrow X$  existiert.

Die Menge  $X$  **besitzt (genau)  $n$  Elemente**, geschrieben  $\#X = n$ , falls eine Bijektion  $\nu: \{1, \dots, n\} \xrightarrow{\sim} X$  existiert (siehe Zählssatz E1G).

Existieren  $n \in \mathbb{N}$  und  $\nu: \{1, \dots, n\} \xrightarrow{\sim} X$ , so nennen wir  $X$  **endlich**, kurz  $\#X < \infty$ , andernfalls nennen wir  $X$  **unendlich**, kurz  $\#X = \infty$ .

Wir nennen  $\#X = |X| = \text{card}(X)$  die **Anzahl der Elemente** von  $X$ , die **Mächtigkeit** der Menge  $X$ , oder die **Kardinalität** der Menge  $X$ .

## Wie viele Elemente hat die vorgelegte Menge?

E114  
Erläuterung

Sei  $n \in \mathbb{N}$ . Als Referenzmenge mit genau  $n$  Elementen nutzen wir hier

$$\underline{n} = \{1, \dots, n\} = \{a \in \mathbb{N} \mid 1 \leq a \leq n\}.$$

😊 Das ist sozusagen das Urmeter, der universelle Maßstab, mit dem wir die Größe einer beliebigen (endlichen) Menge messen.

In John von Neumanns Modell (D125) haben wir noch eleganter

$$n = \{0, 1, \dots, n-1\} = \{a \in \mathbb{N} \mid a < n\}.$$

Hier ist jede natürliche Zahl  $n$  die Menge all ihrer Vorgängerinnen. Zwischen beiden Maßstäben besteht die kanonische Bijektion

$$(s, r) : n \cong \underline{n} : s(a) = a + 1, r(b) = b - 1.$$

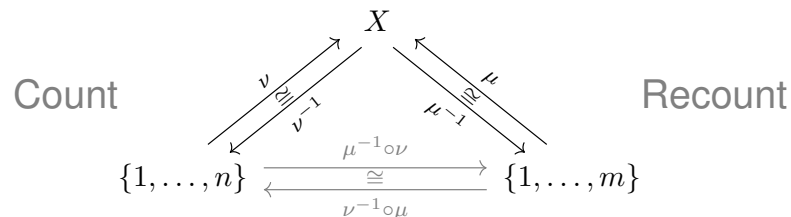
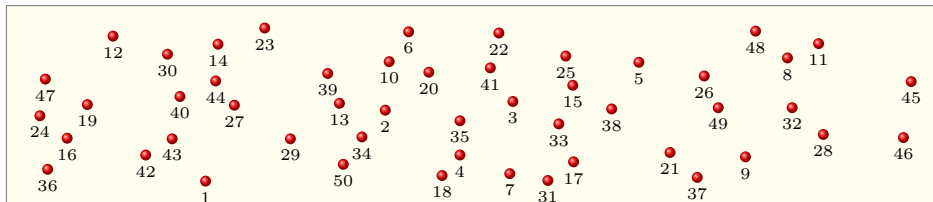
😊 Die Wahl der Referenzmenge ist eine Frage der Tradition und des Geschmacks. Ich nutze meist  $\underline{n}$ , doch manchmal ist  $n$  einfach besser.

Allgemein können wir  $\{a \in \mathbb{Z} \mid m \leq a \leq m + n - 1\}$  nutzen mit  $m \in \mathbb{Z}$ . All diese Maßstäbe stehen kanonisch in Bijektion, alle sind gleich gut.

## Wie viele Elemente hat die vorgelegte Menge?

E115

Wie viele Punkte sehen Sie hier? mindestens? genau?



**Wir hoffen:** Ist  $f: \{1, \dots, n\} \xrightarrow{\sim} \{1, \dots, m\}$  bijektiv, so gilt  $n = m$ . Erst dank dieser Garantie ist die Elementezahl  $\#X$  wohldefiniert!

**Beispiel:** Wie viele Elemente enthält  $X = \{1, \{1\}, \{1, 2\}, \{1, 2, 1\}\}$ ?

## Wie viele Elemente hat die vorgelegte Menge?

E116  
Erläuterung

Wir zählen die Elemente einer beliebigen (endlichen) Menge  $X$ , indem wir willkürlich eine Nummerierung  $\nu: \{1, \dots, n\} \xrightarrow{\sim} X$  wählen. Kommt jede weitere, unabhängige Zählung  $\mu$  zum selben Ergebnis?

Im Beispiel haben wir eine Abzählung  $\nu: \{1, \dots, 50\} \xrightarrow{\sim} X$  gefunden. Genügt vielleicht bereits 49 zu einer Bijektion  $\mu: \{1, \dots, 49\} \xrightarrow{\sim} X$ ? Es gibt  $50! \approx 3 \cdot 10^{64}$  Injektionen, das ist eine astronomisch große Zahl. Es ist praktisch unmöglich, jede einzeln auf Bijektivität zu prüfen!

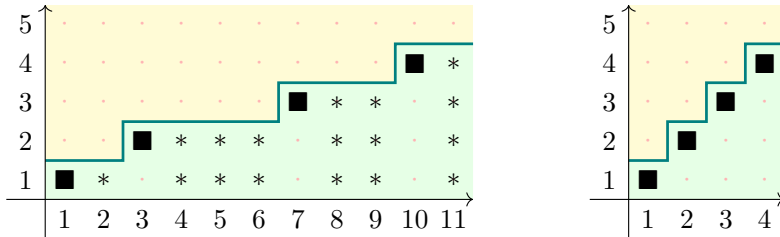
Wir benötigen hier dringend den folgenden grundlegenden **Zählssatz**:

Ist eine Abbildung  $f: \{1, \dots, n\} \xrightarrow{\sim} \{1, \dots, m\}$  bijektiv, so gilt  $n = m$ . Erst dank dieser Garantie ist die Elementezahl  $\#X$  wohldefiniert!

Das ist auch politisch hochaktuell. Alle vier Jahre wird in den USA gewählt und gezählt. . . und nachgezählt! Wir würden hoffen, dass zwei Zählungen derselben Menge immer dasselbe Ergebnis liefern.

Seit Kindheit ist das für Sie eine grundlegende **Erfahrungstatsache**, ebenso wie weitere Rechenregeln (Kommutativität, Assoziativität usw.) Erfahrung ist gut, Intuition ist schön, ein Beweis ist noch besser!

Wir suchen und nutzen die Analogie zum Gauß-Algorithmus B2C:



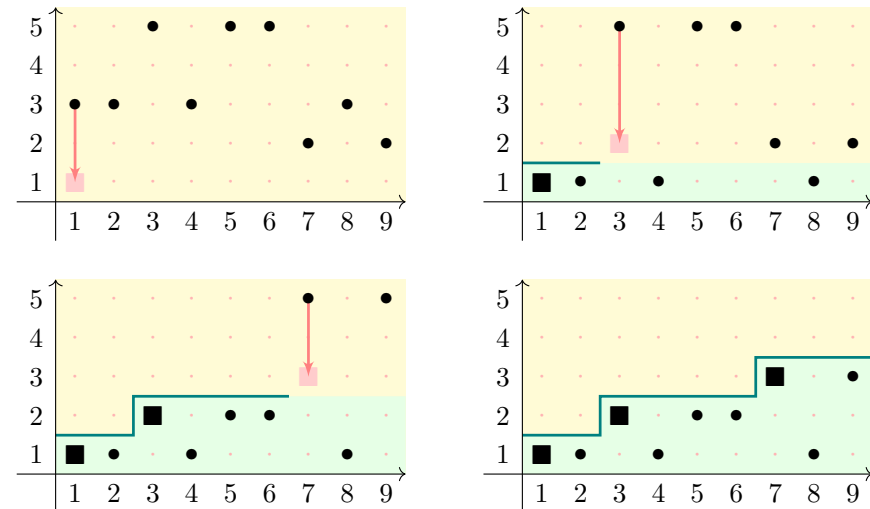
Die Abbildung  $f: \{1, \dots, n\} \rightarrow \{1, \dots, m\}$  ist in **Stufenform**, falls gilt: Wir haben  $\text{im}(f) = \{1, \dots, r\}$  und Stufen  $s_1 < \dots < s_r$  in  $\{1, \dots, n\}$ , an jeder Stufe  $s_k$  gilt  $f(s_k) = k$ , und für alle  $i < s_k$  gilt  $f(i) < k$ .

Insbesondere gilt  $r \leq m$  und  $r \leq n$ . Daraus lesen wir ab:

- Genau dann ist  $f$  surjektiv, wenn  $r = m \leq n$  gilt.
- Genau dann ist  $f$  injektiv, wenn  $r = n \leq m$  gilt.
- Genau dann ist  $f$  bijektiv, wenn  $r = n = m$  gilt.

Im Falle  $r = n$  gilt  $s = (1, 2, \dots, n)$ , also ist  $f = \iota$  die Inklusion / Identität.

Wir können jedes  $f: \{1, \dots, n\} \rightarrow \{1, \dots, m\}$  in Stufenform bringen! Dies gelingt durch Zeilenvertauschung, wie im Gauß-Algorithmus:



Hier ist  $f' = \sigma \circ f$  in Stufenform mit  $\sigma = (3, 5) \circ (2, 5) \circ (1, 3) = (1, 5, 2, 3)$ .

**Lemma E1E: Sortieren zur Stufenform à la Gauß**

Zu jeder Abbildung  $f: \{1, \dots, n\} \rightarrow \{1, \dots, m\}$  existiert eine Zeilenvertauschung  $\sigma \in S_m$ , die  $f' = \sigma \circ f$  in Stufenform bringt.

**Beweis:** Wir sortieren wie im Gauß-Algorithmus B2C:

**Algo E1E: Sortieren zur Stufenform à la Gauß**

**Eingabe:** eine Abbildung  $f: \{1, \dots, n\} \rightarrow \{1, \dots, m\}$

**Ausgabe:** eine Abbildung  $f' = \sigma \circ f$  in Stufenform, wobei  $\sigma \in S_m$   
Genauer gilt  $\sigma = (r, k_r) \circ \dots \circ (2, k_2) \circ (1, k_1)$  mit  $i \leq k_i \leq m$

- 1:  $r \leftarrow 0$ ;  $\sigma = \text{id}$ ;  $s \leftarrow ()$
- 2: **for**  $\ell$  **from** 1 **to**  $n$  **do**
- 3:      $k \leftarrow f(\ell)$
- 4:     **if**  $k > r$  **then**  $r \leftarrow r + 1$ ;  $f \leftarrow (r, k) \circ f$ ;  $\sigma \leftarrow (r, k) \circ \sigma$ ;  $s_r \leftarrow \ell$

Die Permutation  $\sigma$  ist die Komposition der Transpositionen  $(r, k)$ . Das entspricht genau den elementaren Zeilenoperationen bei Gauß. Hier ist alles leichter, denn hier entfällt das Aufräumen der Spalten.

Beachten Sie die wunderschön schöne und erstaunlich präzise Analogie zwischen dem Sortieren von Abbildungen  $f: \{1, \dots, n\} \rightarrow \{1, \dots, m\}$  und dem Gauß-Algorithmus B2C für Matrizen  $A \in \mathbb{K}^{m \times n}$  über einem beliebigen Körper oder Divisionsring  $\mathbb{K}$ :

- Wir können jede Matrix  $A \in \mathbb{K}^{m \times n}$  in Zeilenstufenform  $A' = SA$  bringen durch elementare Zeilenoperationen, zusammengefasst zu einer invertierbaren Matrix  $S \in \text{GL}_m(\mathbb{K})$ .
- Wir können jede Abbildung  $f: \{1, \dots, n\} \rightarrow \{1, \dots, m\}$  in Stufenform  $f' = \sigma \circ f$  bringen allein durch Zeilenvertauschungen, auch diese zusammengefasst zu einer Permutation  $\sigma \in S_m$ .

☺ In beiden Fällen nutzen wir (im Prinzip) denselben Algorithmus: Das grundlegende Gauß-Verfahren für Matrizen  $A$  und ebenso grundlegend (aber einfacher) die Sortierung für Abbildungen  $f$ .

☺ Auch die Folgerungen sind parallel: Die Invertierbarkeitskriterien B2D für Matrizen entsprechen dem folgenden Satz E1F für Abbildungen. Beide sind überaus praktisch, und die Analogie ist bemerkenswert.

**Satz E1F:** Sur/In/Bijektivität von  $f : \{1, \dots, n\} \rightarrow \{1, \dots, m\}$

Vorgelegt sei eine beliebige Abbildung  $f : \{1, \dots, n\} \rightarrow \{1, \dots, m\}$ .  
Wir bringen  $f$  in Stufenform  $f' = \sigma \circ f$  mit Rang  $r \leq \min\{m, n\}$ .

Genau dann ist  $f$  surjektiv / injektiv / bijektiv, wenn dies für  $f'$  gilt:

- (1) Genau dann ist  $f$  surjektiv, wenn  $r = m \leq n$  gilt.
- (2) Genau dann ist  $f$  injektiv, wenn  $r = n \leq m$  gilt.
- (3) Genau dann ist  $f$  bijektiv, wenn  $r = n = m$  gilt.

😊 Das reduziert die Frage auf den Vergleich von drei Kennzahlen!

Zusatz: Ist  $f$  injektiv, so ist  $f' = \iota$  die Inklusion, somit gilt

$$f = (1, k_1) \circ (2, k_2) \circ \dots \circ (n, k_n) \circ \iota$$

mit  $i \leq k_i \leq m$  für alle  $i$ . Dabei ist  $(k_1, k_2, \dots, k_n)$  eindeutig.

In Worten: Jede Injektion bzw. Bijektion  $f : \{1, \dots, n\} \hookrightarrow \{1, \dots, m\}$  schreibt sich eindeutig als Komposition aufsteigender Transpositionen.

😊 Das liefert eine effiziente, eindeutige Darstellung jeder Injektion  $f$ .

**Beweis:** Für  $f'$  in Stufenform sind die Aussagen (1–3) klar.  
Daraus folgen sie für jede Abbildung  $f = \sigma \circ f'$  mit  $\sigma \in S_m$ .

Dank dem Sortierlemma E1E gelten die ersehnten Aussagen daher für *jede beliebige* Abbildung  $f : \{1, \dots, n\} \rightarrow \{1, \dots, m\}$ .

Das Sortierlemma liefert weitere wertvolle Informationen:

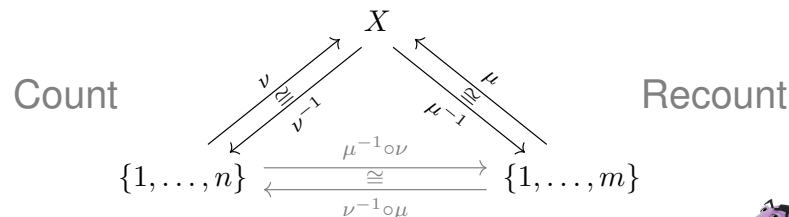
- Rechtsinverse: Ist  $f'$  surjektiv, so ist  $k \mapsto s_k$  eine Rechtsinverse. Jedem Bildwert  $k \in \{1, \dots, m\}$  wird hierdurch sein *erstes* Urbild  $s_k = \min f^{-1}(\{k\})$  zugeordnet. Für  $f = \sigma^{-1} \circ f'$  ist demnach  $g : \{1, \dots, m\} \rightarrow \{1, \dots, n\} : k \mapsto s_{\sigma(k)}$  eine Rechtsinverse.
- Linksinverse: Ist  $f'$  injektiv, so ist  $f$  dank Stufenform immer die Inklusion  $\iota : \{1, \dots, n\} \hookrightarrow \{1, \dots, m\} : i \mapsto i$ . Als Linksinverse wählen wir  $g' : \{1, \dots, m\} \rightarrow \{1, \dots, n\} : j \mapsto \min\{j, n\}$ , sodass  $g' \circ f' = \text{id}$ . Für  $f = \sigma^{-1} \circ f'$  ist demnach  $g = g' \circ \sigma$  eine Linksinverse.

😊 Zudem erhalten wir eine eindeutige Darstellung jeder Injektion  $f$ .

😊 Unsere allgemeinen Sätze zu Abbildungen aus Kapitel D, wie D3A zur Invertierbarkeit, werden für endliche Mengen algorithmisch-konkret!

Warum ist die Elementezahl einer Menge wohldefiniert?

Wir zählen die Elemente einer beliebigen (endlichen) Menge  $X$ , indem wir willkürlich eine Nummerierung  $\nu : \{1, \dots, n\} \xrightarrow{\sim} X$  wählen. Kommt jede weitere, unabhängige Zählung  $\mu$  zum selben Ergebnis?



**Korollar E1G: der Zählssatz**

Seien  $m, n \in \mathbb{N}$  natürliche Zahlen.

- (1) Ist  $f : \{1, \dots, n\} \hookrightarrow \{1, \dots, m\}$  injektiv, so gilt  $n \leq m$ .
- (2) Ist  $f : \{1, \dots, n\} \twoheadrightarrow \{1, \dots, m\}$  surjektiv, so gilt  $n \geq m$ .
- (3) Ist  $f : \{1, \dots, n\} \xrightarrow{\sim} \{1, \dots, m\}$  bijektiv, so gilt  $n = m$ .

Somit ist die Elementezahl  $\#X$  jeder endlichen Menge  $X$  wohldefiniert.



Warum ist die Elementezahl einer Menge wohldefiniert?

Korollar E1G folgt als Satz E1F als **Spezialisierung** der Implikation „ $\Rightarrow$ “  
Die Umkehrung „ $\Leftarrow$ “ gilt in dieser vereinfachten Form hingegen nicht!

- (1) Für  $2 \leq n \leq m$  ist nicht jedes  $f : \{1, \dots, n\} \rightarrow \{1, \dots, m\}$  injektiv!
- (2) Für  $n \geq m \geq 2$  ist nicht jedes  $f : \{1, \dots, n\} \rightarrow \{1, \dots, m\}$  surjektiv!
- (3) Für  $n = m \geq 2$  ist nicht jedes  $f : \{1, \dots, n\} \rightarrow \{1, \dots, m\}$  bijektiv!

Dies sind zunächst nur **notwendige Bedingungen**, sie werden erst hinreichend mit maximalen Rang  $r$ , wie in Satz E1F formuliert.

Bitte vergleichen Sie dies mit dem vollkommen analogen Satz B2D:  
Gegeben sei eine Matrix  $A \in \mathbb{K}^{m \times n}$  über einem Körper / Divisionsring  $\mathbb{K}$ .  
Dazu bringen wir  $A$  auf Zeilenstufenform  $A'$ , mit Rang  $r \leq \min\{m, n\}$ .  
Für die zugehörige Abbildung  $f : \mathbb{K}^n \rightarrow \mathbb{K}^m : x \mapsto Ax$  gilt dann:

- (1) Genau dann ist  $f$  surjektiv, wenn  $r = m \leq n$  gilt.
- (2) Genau dann ist  $f$  injektiv, wenn  $r = n \leq m$  gilt.
- (3) Genau dann ist  $f$  bijektiv, wenn  $r = m = n$  gilt.

Auch hier sind  $n \geq m / n \leq m / n = m$  nur notwendige Bedingungen für die Sur/In/Bijektivität von  $f$ , hinreichend erst mit maximalem Rang  $r$ .

Ich erkläre dieses fundamentale Ergebnis hier bewusst ausführlich. Auf den ersten Blick mag das übertrieben erscheinen. Ich habe Gründe:

- Es handelt sich um eine grundlegende Aussage über Bijektionen. Für eine Einführung in die Mathematik ist dies also eine gute Übung.
- Die Analogie zwischen Gauß und Sortierung ist bemerkenswert. Diese Parallelen erklären gegenseitig und fördern das Verständnis.
- Sie sollen lernen, präzise zu formulieren und kritisch zu denken. Das erfordert ausgiebige Übung und manchmal auch Überwindung. Daher scheint es geboten, in einfachen Fällen damit anzufangen.

Ihnen begegnen in der Mathematik sehr oft analoge Situationen:

- Ist „die Lösung“ einer gegebenen Gleichung wohldefiniert?
- Ist die Dimension eines Vektorraums  $V$  über  $\mathbb{K}$  wohldefiniert?
- Ist das Volumen / Maß einer Menge  $A \subseteq \mathbb{R}^n$  wohldefiniert?
- Ist die Euler–Charakteristik eines Polyeders wohldefiniert?

Dahinter steckt ein Grundprinzip: Existenz und Eindeutigkeit! Sie wollen ein Problem zunächst präzise beschreiben und definieren, was Sie als Lösung zulassen. Anschließend möchten Sie im Idealfall garantieren, dass eine Lösung existiert und zudem eindeutig ist. (Das ist nicht immer möglich, aber es ist das ersehnte Ideal.)

Alle Rechenaufgaben, selbst einfache, beruhen auf diesem Prinzip: Ist „das Ergebnis“ eindeutig, wohldefiniert, unabhängig vom Rechenweg? Wir müssten sonst befürchten, dass auf dem einen Rechenweg „das“ Ergebnis  $E = 42$  berechnet wird, auf einem anderen Rechenweg jedoch „das“ Ergebnis  $E = 43$ . Unsere Definition / Aufgabenstellung / Frage wäre dann in sich widersprüchlich und somit wertlos.

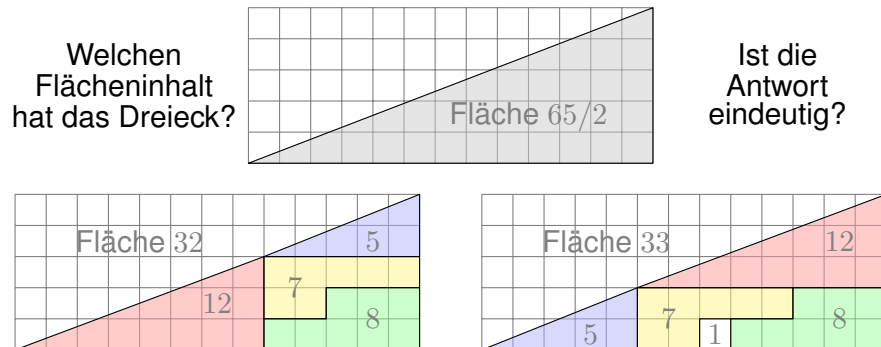
Solche warnenden Beispiele begegnen uns tatsächlich häufig!

*The method of postulating what we want has many advantages; they are the same as the advantages of theft over honest toil.*  
Bertrand Russell, 1872–1970, *Introduction to Mathematical Philosophy*

Wir können jeder messbaren Menge  $A \subset \mathbb{R}^2$  ihren Flächeninhalt  $\text{vol}_2(A)$  zuordnen, etwa Rechtecken, Dreiecken, Polygonen, etc.

Es ist bemerkenswert, dass das Ergebnis immer eindeutig ist, insbesondere unabhängig vom Rechenweg! Oder etwa doch nicht?

Wir zerlegen das rechtwinklige Dreieck  $\Delta$  mit Kathetenlängen 13 und 5 wie skizziert und berechnen den Flächeninhalt  $\text{vol}_2(\Delta)$  auf drei Weisen:



**Lösung:** Die links gezeigten Mengen nennen wir  $A_5, A_7, A_8, A_{12}$ . Jede hat den angegebenen Flächeninhalt  $\text{vol}_2(A_k) = k$ . Je zwei sind fast disjunkt: Ihr Schnitt hat Flächeninhalt  $\text{vol}_2(A_k \cap A_l) = 0$  für  $k \neq l$ . Dank unserer Rechenregeln erhalten wir für  $A = A_5 \cup A_7 \cup A_8 \cup A_{12}$  demnach den Flächeninhalt  $\text{vol}_2(A) = 5 + 7 + 8 + 12 = 32$ .

Auf der rechten Seite betrachten wir entsprechend die Mengen  $B_1, B_5, B_7, B_8, B_{12}$ . Für ihre Vereinigung  $B = B_1 \cup B_5 \cup B_7 \cup B_8 \cup B_{12}$  erhalten wir nach denselben Regeln  $\text{vol}_2(B) = 1 + 5 + 7 + 8 + 12 = 33$ .

Für das Dreieck  $\Delta$  hingegen erhalten wir  $\text{vol}_2(\Delta) = 65/2 = 32.5$ . Wir erhalten auf drei Rechenwegen also drei verschiedene Ergebnisse! Ist der Flächeninhalt also in Wirklichkeit gar nicht wohldefiniert?

Was geht hier schief? Die Skizze suggeriert  $A = \Delta = B$  und provoziert den Widerspruch. Bei genauem Hinsehen erkennen Sie  $A \subsetneq \Delta \subsetneq B$ . Diese Einschachtelung zeigt  $\text{vol}_2(A) = 32 \leq \text{vol}_2(\Delta) \leq 33 = \text{vol}_2(B)$ .

Alles wird gut! Der Flächeninhalt  $\text{vol}_2$  im  $\mathbb{R}^2$  und das Volumen  $\text{vol}_n$  im  $\mathbb{R}^n$  ist tatsächlich wohldefiniert. Freuen Sie sich auf das Lebesgue–Maß!



**Satz E1H: Invarianz der Elementezahl**

Seien  $X$  und  $Y$  endliche Mengen und  $f: X \rightarrow Y$  eine Abbildung. Für  $r = \# \text{im}(f)$  gilt dann  $r \leq \#X$  und  $r \leq \#Y$ , also  $r \leq \min\{\#X, \#Y\}$ .

- (1) Genau dann ist  $f$  surjektiv, wenn  $r = \#Y \leq \#X$  gilt.
- (2) Genau dann ist  $f$  injektiv, wenn  $r = \#X \leq \#Y$  gilt.
- (3) Genau dann ist  $f$  bijektiv, wenn  $r = \#X = \#Y$  gilt.

Als Spezialisierung erhalten wir insbesondere:

$$\begin{array}{ccc}
 X & \xrightarrow{f} & Y \\
 \nu \uparrow \cong \downarrow \nu^{-1} & & \mu \uparrow \cong \downarrow \mu^{-1} \\
 \{1, \dots, n\} & \xrightarrow{g} & \{1, \dots, m\}
 \end{array}$$

(1') Ist  $f: X \xrightarrow{\sim} Y$  bijektiv, so gilt  $\#X = \#Y$ .  
 (2') Ist  $f: X \twoheadrightarrow Y$  surjektiv, so gilt  $\#X \geq \#Y$ .  
 (3') Ist  $f: X \hookrightarrow Y$  injektiv, so gilt  $\#X \leq \#Y$ .

Per Kontraposition folgt aus (3') sofort:

**Korollar E1I: Dirichlets Schubfachprinzip**

Sei  $f: X \rightarrow Y$  eine Abbildung. Gilt  $\#X > \#Y$ , so ist  $f$  nicht injektiv: Es existieren zwei Elemente  $a \neq b$  in  $X$  mit  $f(a) = f(b)$  in  $Y$ .

Das Schubfachprinzip ist ein einfacher und eleganter **Existenzbeweis**. Trotz seiner Einfachheit hilft Ihnen dieses Prinzip erstaunlich oft! Ehrlicherweise, sollte ich aber auch sagen, was es nicht leistet:

Es sagt uns nicht, *wie* wir ein solches Paar  $a \neq b$  in  $X$  mit  $f(a) = f(b)$  effizient finden, es garantiert nur, *dass* es ein solches Paar gibt.

Eine solche reine Existenzaussage ist zwar leider nicht konstruktiv, doch oft ist eine schwache Aussage besser als gar keine Aussage. Sie ist nicht das Ende der Problemlösung, sondern ein guter Anfang.

Die Existenz einer Lösung hilft in vielen praktischen Anwendungen: Bevor Sie sich auf die lange und mühevollen Suche nach einer Lösung begeben, wollen Sie sicher sein, dass sich Ihre Mühe auch lohnen wird.

Oder noch extremer: Es ist ganz sicher besser frühzeitig zu erkennen, dass es keine Lösung gibt, als jahrelang vergeblich danach zu suchen. Das nachfolgende Beispiel E1K illustriert dies eindrücklich, als Video von Burkard Polster, *The pigeon hole principle*, [youtu.be/TCZ3YwbcDaw](https://youtu.be/TCZ3YwbcDaw).

Sie bestaunen hier die erste und wichtigste Invariante der Mathematik: Die Elementezahl ändert sich nicht unter Anwendung von Bijektionen!

Allgemein versteht die Mathematik unter einer **Invariante** folgendes: Jedem der betrachteten Objekte (hier: endliche Mengen) wird eine Größe zugeordnet (hier: ihre Elementezahl); diese Größe ändert sich nicht unter den betrachteten Umformungen (hier: alle Bijektionen).

Invarianten sind ein wichtiges Hilfsmittel bei Klassifikationsproblemen: Objekte mit unterschiedlichen Invarianten sind wesentlich verschieden. Manchmal gilt sogar die Umkehrung, und Objekte mit gleichen Werten unter der Invariante lassen sich ineinander umformen. Wir sprechen dann von einer **vollständigen Invarianten**. Genau das liegt hier vor:

**Korollar E1J: Klassifikation endlicher Mengen bis auf Bijektion**

Zwei endliche Mengen  $X$  und  $Y$  stehen genau dann in Bijektion, kurz  $X \cong Y$ , wenn sie dieselbe Elementezahl haben, kurz  $\#X = \#Y$ .

☺ Wir sehen dieses Prinzip immer wieder, etwa in Satz J2J bei der Klassifikation endlich-dimensionaler Vektorräume bis auf Isomorphie.

**Behauptung:** Es gibt in Stuttgart mindestens zwei Personen, die exakt dieselbe Anzahl von Haaren auf dem Kopf haben.

**Beweis:** Typischerweise hat ein Mensch 100 000 bis 200 000 Haare, sicher weniger als 500 000. Stuttgart hat knapp über 635 000 Einwohner. Somit ist die Haarzahl  $h: \{\text{Einwohner}\} \rightarrow \{0, \dots, 500000\}$  nicht injektiv.

☺ Das ist ein eleganter Existenzbeweis, wenn auch nicht konstruktiv. Er sagt uns, *dass* wir ein solches Paar finden können, aber nicht *wie*!

Mit solchen Formulierungen lässt sich das Schubfachprinzip schön illustrieren und auch leicht merken. Natürlich gibt es hier zahlreiche mögliche Einwände, wie immer bei allzu anschaulichen Beispielen. Ist die Haarzahl genau bestimmt? Können wir sie praktisch zählen?

Das ist keine ernsthafte *Anwendung*, sondern eher eine scherzhafte *Illustration*. Da es in Stuttgart mindestens zwei Kahlköpfige gibt, ist die hier gemachte Aussage ohnehin trivial. Aber Sie verstehen das Prinzip.

☺ Die folgende schöne Anwendung ist rein mathematisch, daher viel einfacher, und über jede Haarspalterei erhaben.

**Aufgabe:** Wir nennen  $T \subseteq \mathbb{N}$  **teilerfrei**, falls  $s \nmid t$  für alle  $s \neq t$  in  $T$  gilt.

- (1) Finden Sie eine teilerfreie Menge  $T \subseteq \{1, \dots, 100\}$  mit  $\#T = 50$ .
- (2) Finden Sie alle teilerfreien Mengen  $T \subseteq \{1, \dots, 100\}$  mit  $\#T = 51$ .

**Lösung:** (1) Die Menge  $T = \{51, \dots, 100\}$  ist teilerfrei. (2) Es gibt keine! Allgemein gilt hierzu das folgende bemerkenswert elegante Ergebnis:

#### Beispiel E1K: Anwendung des Schubfachprinzips

Wir betrachten  $V = \{1, \dots, 2n\}$  mit  $n \in \mathbb{N}_{\geq 1}$ . Sei  $T \subseteq V$  mit  $\#T > n$ . Dann existiert mindestens ein Paar  $s \neq t$  in  $T$  mit  $s \mid t$ .

**Beweis:** Die Menge  $U := \{1, 3, 5, \dots, 2n-1\}$  hat genau  $n$  Elemente. Wir definieren die Abbildung  $f: V \rightarrow U: x \mapsto x'$  durch  $x = 2^k x'$ ,  $k \in \mathbb{N}$ . Wegen  $\#T > \#U$  ist  $f|_T: T \rightarrow U$  nicht injektiv dank Schubfachprinzip E1I. Also existieren zwei verschiedene Elemente  $s < t$  in  $T$  mit  $f(s) = f(t)$ . Für diese gilt  $s = 2^k s'$  und  $t = 2^\ell s'$  mit  $k < \ell$ , und somit  $s \mid t$ . QED

😊 Das ist ein eleganter Existenzbeweis! Wir müssen nur noch suchen. Der Beweis garantiert, dass wir ein solches Paar in  $T$  finden werden. Anschließend können wir nach effizienten Algorithmen fragen. . . Auch dies ist im vorliegenden Beispiel erfreulich einfach.

Schon die „reine Existenzaussage“ ist hier bereits extrem hilfreich! Die ursprüngliche, ganz praktische Aufgabenstellung lautet ja: Finden Sie alle teilerfreien Mengen  $T \subseteq \{1, \dots, 100\}$  mit  $\#T = 51$ .

Naiv müsste man sich nun daran machen, alle möglichen Teilmengen  $T \subseteq \{1, \dots, 100\}$  durchzuprobieren, um nur die teilerfreien zu behalten. Schon in diesem kleinen Beispiel ist dies eine lange und mühselige Arbeit: „Die Guten ins Töpfchen, die Schlechten ins Kröpfchen“

Das Schubfachprinzip liefert hier eine schnelle und präzise Antwort: Es gibt keine einzige teilerfreie Menge  $T \subseteq \{1, \dots, 100\}$  mit  $\#T = 51$ . Damit haben wir unsere Suche schnell und vollständig durchgeführt. Es lohnt sich daher, in gute Denkwerkzeuge zu investieren.

Ein **Integritätsring**  $(R, +, 0, \cdot, 1)$  ist ein kommutativer Ring mit  $1 \neq 0$  ohne Nullteiler. Letzteres heißt: Für alle  $a, b \neq 0$  in  $R$  gilt  $a \cdot b \neq 0$ .

**Beispiele:** Jeder Körper ist ein Integritätsring, etwa  $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p$ . Die ganzen Zahlen  $\mathbb{Z}$  sind ein Integritätsring, aber kein Körper. Der Ring  $\mathbb{Z}_6$  hingegen hat Nullteiler, denn hier gilt  $2 \cdot_6 3 = 0$ . Die Ringe  $\mathbb{Z}_5$  und  $\mathbb{Z}_7$  sind nullteilerfrei. . . und Körper!

#### Satz E1L: endliche Integritätsringe

Jeder endliche Integritätsring  $(R, +, 0, \cdot, 1)$  ist ein Körper.

**Beweis:** Zu  $a \in R \setminus \{0\}$  betrachten wir die Linksmultiplikation

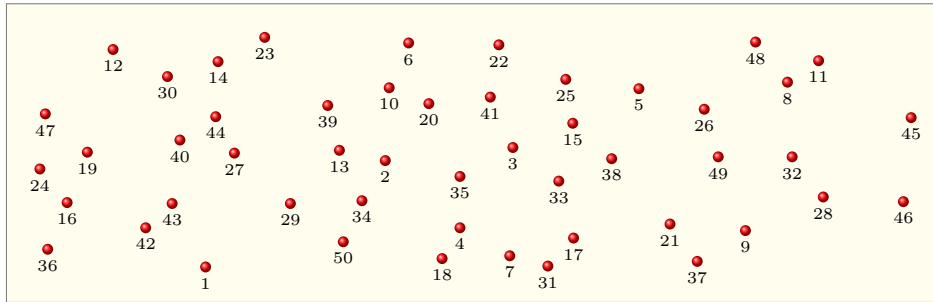
$$\lambda_a : R \rightarrow R : x \mapsto a \cdot x.$$

Diese ist injektiv: Aus  $a \cdot x = a \cdot x'$  folgt  $a \cdot (x - x') = 0$ , also  $x = x'$ . Die Menge  $R$  ist endlich, also ist  $\lambda_a$  auch surjektiv dank Satz E1H. Insbesondere existiert zur Gleichung  $a \cdot x = 1$  eine Lösung  $x \in R$ . Somit ist jedes Element  $a \neq 0$  in  $R$  invertierbar. QED

😊 Aus geringen Voraussetzungen erhalten wir starke Folgerungen, allein dank der Endlichkeit der Menge  $R$ ! Das ist bemerkenswert. Es ist eine erste frappierende Anwendung des Invarianzsatzes E1H. Für endliche Mengen und ihre Abbildungen gelten besonders starke und nützliche Gesetzmäßigkeiten: *Defendit numerus*. [Die Zahl gibt Schutz.] Dies wollen und werden wir im Folgenden immer wieder nutzen.

Auch für unendliche Mengen gelten nützliche Gesetzmäßigkeiten, wenn auch deutlich andere und manchmal schockierend paradox. Damit werden wir uns im folgenden Kapitel genauer beschäftigen.

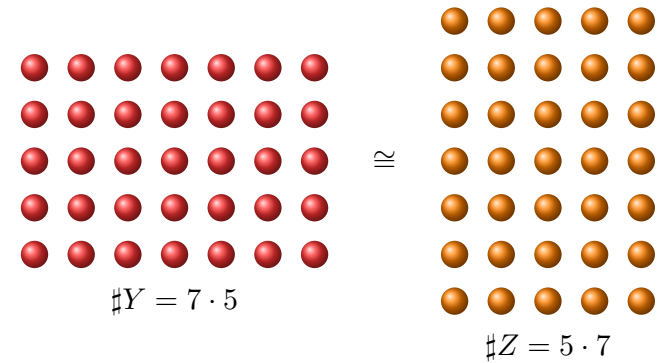
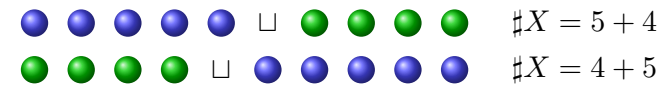
In diesem Kapitel geht es zunächst um endliche Mengen und die hierbei geltenden Abzählregeln. Vieles davon wird Ihnen sofort einleuchten, vermutlich gar trivial vorkommen. Das ist gut, schauen Sie genau hin! Ich führe hier bewusst alle Details explizit aus: Es ist eine gute Übung in präziser Formulierung und Argumentation. Zudem bereitet es Sie auf unendliche Mengen vor, die sich deutlich anders verhalten.



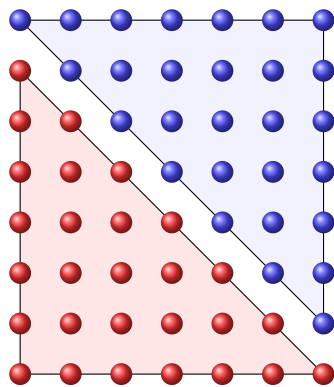
Das Zählen von Dingen ist *die* mathematische Grunderfahrung, sowohl psychologisch-individuell als auch historisch-gesellschaftlich. Das Abzählen spielt eine zentrale Rolle in nahezu jeder Anwendung der Mathematik, vom alltäglichen Handel und Wandel zur Quantenmechanik.

Mengen sind konkret, Zahlen sind abstrakt. Daher nutzt die Didaktik gezielt Mengen, um das Rechnen mit Zahlen zu veranschaulichen. Viele der folgenden Ergebnisse kommen Ihnen daher bekannt vor. Was für Sie neu hinzukommt, ist der formal mathematische Rahmen.

Wir wollen strukturierte Mengen effizient abzählen. Mengenoperationen entsprechen dabei wunderbar Rechenoperationen natürlicher Zahlen:



$$1 + 2 + 3 + \dots + n =: S(n)$$



$$2S(n) = n(n + 1)$$

Dieses genial-einfache Argument zeigt die geschlossene Formel

$$\sum_{k=1}^n k = \frac{n(n + 1)}{2}.$$

Dahinter stecken einfache Regeln, die wir hier explizit benennen:

- 1 Doppeltes Abzählen einer Menge ergibt dieselbe Elementezahl in  $\mathbb{N}$ .
- 2 Daraus folgt die Invarianz: Jede Bijektion erhält die Elementezahl.
- 3 Disjunkte Vereinigung von Mengen entspricht der Summe in  $\mathbb{N}$ .
- 4 Kartesisches Produkt von Mengen entspricht dem Produkt in  $\mathbb{N}$ .

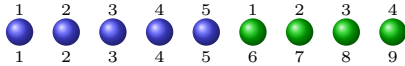
Wir wenden dies wie folgt an – meist unbewusst, hier explizit:

- Das blaue Dreieck  $\Delta$  hat genau  $S(n)$  Elemente dank (3).
- Wir drehen das blaue in das rote Dreieck  $\Delta'$  und nutzen (2).
- Das Rechteck  $R$  ist disjunkte Vereinigung der beiden Dreiecke (3).
- Die Elementezahl des Rechtecks ist das Produkt  $n(n + 1)$  dank (4).

Wir zählen das Rechteck somit auf zwei Arten (1) und erhalten

$$R = \Delta \sqcup \Delta' \implies n(n + 1) = S(n) + S(n).$$

Umgestellt erhalten wir die ersehnte Formel  $S(n) = n(n - 1)/2$ .



**Satz E2A: Mächtigkeit einer disjunkten Vereinigung**

Seien  $X$  und  $Y$  endliche Mengen mit  $X \cap Y = \emptyset$ . Dann gilt:

$$\#(X \sqcup Y) = (\#X) + (\#Y)$$

Explizite Konstruktion: Gegeben seien die Abzählungen

$$\begin{aligned} \mu &: \{1, \dots, p\} \xrightarrow{\sim} X, \\ \nu &: \{1, \dots, q\} \xrightarrow{\sim} Y. \end{aligned}$$

Daraus konstruieren wir die Abzählung der disjunkten Vereinigung

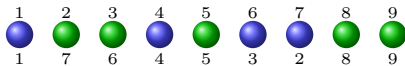
$$(\sigma, \tau) : \{1, \dots, p+q\} \cong X \sqcup Y$$

durch  $\sigma(k) = \mu(k)$  für  $1 \leq k \leq p$  und  $\sigma(k) = \nu(k-p)$  für  $p < k \leq p+q$  sowie  $\tau(x) = \mu^{-1}(x)$  für  $x \in X$  und  $\tau(y) = \nu^{-1}(y) + p$  für  $y \in Y$ .

Tatsächlich ist  $(\sigma, \tau)$  eine Bijektion. Die Formeln liegen explizit vor, es genügt also nachzurechnen, dass  $\tau \circ \sigma = \text{id}$  und  $\sigma \circ \tau = \text{id}$  gilt. Dies beweist die behauptete Gleichung zwischen den Elementzahlen. Es gibt viele Abzählungen, aber das Ergebnis ist eindeutig, siehe E1G.

Ist das nicht irgendwie intuitiv klar? Müssen wir es explizit konstruieren? Ja, wenn es so klar ist, dann können wir es leicht explizit konstruieren! Ist das übertrieben pedantisch? Nein, die Abzählung E1D verlangt eine Bijektion, also sollten wir eine konkrete Bijektion vorweisen.

Dasselbe gilt insbesondere im folgenden Fall einer Teilmenge  $X \subseteq Z$ . Natürlich ist intuitiv klar, dass  $\#X \leq \#Z$  und  $\#(Z \setminus X) = (\#Z) - (\#X)$  gilt. Aber woher bekommen wir eine geeignete Abzählung, die das belegt? Ganz einfach: Wir müssen sie konstruieren! Es ist zum Glück leicht.



**Satz E2B: Mächtigkeit von Teilmengen und Vereinigungen**

(0) Ist  $Z$  endlich, so auch jede Teilmenge  $X \subseteq Z$ . Genauer gilt:

$$X \subseteq Z \implies \#X \leq \#Z, \quad \#(Z \setminus X) = (\#Z) - (\#X)$$

Explizite Konstruktion: Sei  $\nu : \{1, \dots, n\} \xrightarrow{\sim} Z$  eine Abzählung. Zu jeder Zerlegung  $Z = X \sqcup Y$  existiert eine Sortierung  $\sigma \in S_n$  zu einer angepassten Abzählung  $\mu = \nu \circ \sigma : \{1, \dots, n\} \xrightarrow{\sim} Z$  mit  $\mu(\{1, \dots, p\}) = X$  und  $\mu(\{p+1, \dots, n\}) = Y$ .

(1) Für beliebige endliche Mengen  $X, Y$  folgt daraus:

$$\#(X \cup Y) = \#X + \#Y - \#(X \cap Y)$$

Explizite Konstruktion: Es gilt  $X \cup Y = X \sqcup Y'$  mit  $Y' = Y \setminus (X \cap Y)$ .

Die Aussage  $\#X \leq \#Z$  folgt bereits aus der Invarianz E1H dank Inklusion  $\iota : X \hookrightarrow Z$ . Auch die Sortierung von  $\nu$  zum angepassten  $\mu$  folgt aus dem Sortierlemma E1E. Ich führe es zur Deutlichkeit hier unabhängig aus.

**Beweis:** (0) Wir können  $X \subseteq Z$  nach vorne sortieren:

**Algo E2B: Sortiere  $X \subseteq Z$  nach vorne**

**Eingabe:** Abzählung  $\nu : \{1, \dots, n\} \xrightarrow{\sim} Z$  und Zerlegung  $Z = X \sqcup Y$

**Ausgabe:**  $(\mu, \sigma, p)$  mit  $\mu = \nu \circ \sigma$  und  $\sigma \in S_n$  und  $\mu(\{1, \dots, p\}) = X$

```

1:  $q \leftarrow 1; p \leftarrow n; \mu \leftarrow \nu; \sigma \leftarrow \text{id}$  //  $\mu(\{1, \dots, q-1\}) \subseteq X$ 
2: while  $q \leq p$  do //  $\mu(\{p+1, \dots, n\}) \subseteq Y$ 
3:   while  $q \leq n \wedge \mu(q) \in X$  do  $q \leftarrow q + 1$  // erstes Element in  $Y$ 
4:   while  $p \geq 1 \wedge \mu(p) \in Y$  do  $p \leftarrow p - 1$  // letztes Element in  $X$ 
5:   if  $q < p$  then  $\mu \leftarrow \mu \circ (q, p); \sigma \leftarrow \sigma \circ (q, p)$  // tausche falls nötig
6: return  $(\mu, \sigma, p)$  // nun liegt  $X$  vor  $Y$ 
    
```

(1) Wir zerlegen  $X \cup Y = X \sqcup Y'$  mit  $Y' = Y \setminus (X \cap Y)$ . Dank Satz E2A und (0) folgt  $\#(X \cup Y) = \#X + \#Y' = \#X + \#Y - \#(X \cap Y)$ . QED

**Beispiel:** Wir wollen kartesische Produkte  $X \times Y$  abzählen.  
Konkret betrachten wir  $X = \{0, \dots, p-1\}$  und  $Y = \{0, \dots, q-1\}$ .

3	(0, 3) → 21	(1, 3) → 22	(2, 3) → 23	(3, 3) → 24	(4, 3) → 25	(5, 3) → 26	(6, 3) → 27
2	(0, 2) → 14	(1, 2) → 15	(2, 2) → 16	(3, 2) → 17	(4, 2) → 18	(5, 2) → 19	(6, 2) → 20
1	(0, 1) → 7	(1, 1) → 8	(2, 1) → 9	(3, 1) → 10	(4, 1) → 11	(5, 1) → 12	(6, 1) → 13
0	(0, 0) → 0	(1, 0) → 1	(2, 0) → 2	(3, 0) → 3	(4, 0) → 4	(5, 0) → 5	(6, 0) → 6
	0	1	2	3	4	5	6

Zeilenweises Abzählen ergibt  $(f, g) : X \times Y \cong \{0, \dots, pq-1\}$   
mit  $f(x, y) = x + yp$  und Umkehrung  $g(z) = (z \text{ rem } p, z \text{ quo } p)$ .  
Das ist tatsächlich eine Bijektion, denn  $g \circ f = \text{id}$  und  $f \circ g = \text{id}$ .

**M** Dies iteriert Satz E2A für  $X \times Y = X \times \{0\} \sqcup \dots \sqcup X \times \{p-1\}$ :  
Wir legen die Zeilen hintereinander. (Genauso gelingt es mit Spalten.)

**I** Auf dem Computer werden Matrizen so konsekutiv gespeichert.  
Unsere konkrete Indexumrechnung ist dabei überaus praktisch.

## Satz E2C: Mächtigkeit eines kartesischen Produkts

Seien  $X$  und  $Y$  endliche Mengen. Dann gilt:

$$\#(X \times Y) = (\#X) \cdot (\#Y)$$

Explizite Konstruktion: Gegeben seien

$$\mu : \{0, \dots, p-1\} \xrightarrow{\sim} X,$$

$$\nu : \{0, \dots, q-1\} \xrightarrow{\sim} Y.$$

Daraus konstruieren wir die Abzählung des Produkts

$$(\sigma, \tau) : \{0, \dots, pq-1\} \cong X \times Y$$

durch  $\sigma(z) = (\mu(z \text{ rem } p), \nu(z \text{ quo } p))$  und  $\tau(x, y) = \mu^{-1}(x) + \nu^{-1}(y)p$ .

**Übung:** Das ist tatsächlich eine Bijektion, denn  $\tau \circ \sigma = \text{id}$  und  $\sigma \circ \tau = \text{id}$ .  
Stehen die Abbildungen erst einmal vor uns, so genügt Nachrechnen!  
Ich betone nochmal: Explizite Formeln sind nicht Fluch, sondern Segen.

## Satz E2D: Mächtigkeit von Summen und Produkten

Für (disjunkte) Mengen  $X_1, X_2, \dots, X_n$  gilt:

$$X_1 \sqcup X_2 \sqcup \dots \sqcup X_n = (X_1 \sqcup X_2 \sqcup \dots) \sqcup X_n$$

$$X_1 \times X_2 \times \dots \times X_n = (X_1 \times X_2 \times \dots) \times X_n$$

Aus den Sätzen E2B und E2C folgt damit per Induktion:

$$\#(X_1 \sqcup X_2 \sqcup \dots \sqcup X_n) = (\#X_1) + (\#X_2) + \dots + (\#X_n).$$

$$\#(X_1 \times X_2 \times \dots \times X_n) = (\#X_1) \cdot (\#X_2) \cdot \dots \cdot (\#X_n).$$

**Übung:** (0) Warum gelten die gezeigten Gleichungen für die Mengen?  
(1) Beweisen Sie die zugehörigen Gleichungen für die Elementezahlen.  
(2) Konstruieren Sie auch hier möglichst explizite Abzählungen.

**Lösung:** (0) Die erste Gleichheit für die disjunkte Summe ist klar:

$$X_1 \sqcup X_2 \sqcup \dots \sqcup X_n = (X_1 \sqcup X_2 \sqcup \dots) \sqcup X_n$$

Die zweite Gleichheit verdanken wir unserer Definition (Seite D138)  
des  $n$ -fachen kartesischen Produkts durch Linksklammerung:

$$X_1 \times X_2 \times \dots \times X_n = (X_1 \times X_2 \times \dots) \times X_n$$

Andernfalls stünde hier statt strikter Gleichheit „ $\cong$ “ eine geeignete  
Bijektion „ $\cong$ “ durch Umklammerung, siehe Seite E223 für ein Beispiel.  
Dank Invarianz E1H wäre jede Bijektion für unsere Zwecke genauso gut.

(1) Für  $n = 1$  ist die jeweilige Aussage  $X_1 = X_1$  und  $\#X_1 = \#X_1$  trivial.  
Der Fall  $n = 2$  wurde in Satz E2A und E2C konstruktiv ausgeführt.  
Diese Konstruktion setzt sich per Induktion für alle  $n \in \mathbb{N}$  fort.

(2) Explizite Abzählungen erhalten wir genau nach obiger Vorlage.  
Für das Produkt nutzen wir die Zifferndarstellung in gemischter Basis.

Als Spezialfall des vorigen Satzes E2D erhalten wir  $\#(X^n) = (\#X)^n$ . Wir betrachten diesen Fall hier noch etwas ausführlicher, da Potenzen dieser Art häufig auftreten und zudem interessante Formeln liefern.

**Beispiel:** Wir wollen kartesische Potenzen  $X^n$  abzählen. Konkret betrachten wir hierzu die Menge  $X = \{0, \dots, p-1\}$ .

Wir nutzen die Zifferndarstellung in Basis  $p$  (Satz A2B):

$$\begin{aligned} (f, g) : \{0, \dots, p-1\}^n &\cong \{0, \dots, p^n-1\}, \\ f(z_0, z_1, \dots, z_{n-1}) &= z_0 + z_1 p + \dots + z_{n-1} p^{n-1}, \\ g(z) &= (z_0, z_1, \dots, z_{n-1}) \quad \text{mit} \quad z_k = (z \text{ quo } p^k) \text{ rem } p. \end{aligned}$$

**M** Die Iteration von Satz E2c ergibt die Zifferndarstellung zur Basis  $p$ . Auch hier ist es besser, bei 0 anzufangen, das vereinfacht die Formeln.

### Satz E2E: Mächtigkeit einer kartesischen Potenz

Sei  $X$  eine endliche Menge und  $n \in \mathbb{N}$ . Dann gilt:

$$\#(X^n) = (\#X)^n$$

Explizite Konstruktion: Gegeben sei eine Abzählung

$$\mu : \{0, \dots, p-1\} \xrightarrow{\sim} X.$$

Daraus konstruieren wir die Abzählung der Potenz

$$(\sigma, \tau) : \{0, \dots, p^n-1\} \cong X^n$$

durch  $\sigma(z) = (x_0, x_1, \dots, x_{n-1})$  mit  $x_k = \mu((z \text{ quo } p^k) \text{ rem } p)$  und  $\tau(x_0, x_1, \dots, x_{n-1}) = \mu^{-1}(x_0) + \mu^{-1}(x_1)p + \dots + \mu^{-1}(x_{n-1})p^{n-1}$ .

Auf den ersten Blick mutet es an wie ein Wunder, dass sich die Mengenoperationen  $X \sqcup Y$  und  $X \times Y$  und  $X^n$  so nahtlos übersetzen in die Zahlenoperationen  $x + y$  und  $x \cdot y$  und  $x^n$ . Dieses „Wunder“ hat jedoch eine einfache Erklärung: Die natürlichen Zahlen wurden gerade dafür geschaffen, um solche Phänomene arithmetisch abzubilden.

In der Entwicklung der Menschheit scheint dies recht plausibel: Zuerst gab es die Objekte selbst, dann erst wurden sie gezählt. Gerade Vereinigung und Produkt treten im Alltag häufig auf, und die Zahlen wurden entwickelt, dies wiederzugeben.

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

In Anbetracht der obigen Zählformeln bin ich versucht zu sagen:  
Die Mengen sind das Urmaterial, alles andere ist Menschenwerk.

Egal ob zahlenmystisches Wunder oder historisch erklärbar, freuen wir uns an diesem harmonischen Zusammenklang!

Auf der einen Seite haben wir endliche Mengen und ihre Abbildungen, auf der anderen Seite haben wir die vertrauten natürlichen Zahlen.

In manchen Fällen sind die Zahlen einfacher: Wir begnügen uns dann mit der Anzahl der Elemente und vernachlässigen die Menge selbst.

In anderen Fällen ist die dahinterliegende Menge einfacher oder informativer, dann lohnt es sich, die reichere Struktur zu nutzen.

Die Menge aller Abbildungen von  $X$  nach  $Y$  bezeichnen wir mit

$$\text{Abb}(X, Y) := \{ f : X \rightarrow Y \} = Y^X.$$

**Beispiel Zahlenschloss:** Wie viele Abbildungen  $f : X \rightarrow Y$  gibt es von der Startmenge  $X = \{1, 2, 3, 4\}$  in die Zielmenge  $Y = \{0, 1, \dots, 9\}$ ?

### Satz E2F: Mächtigkeit der Abbildungsmenge

Sind  $X$  und  $Y$  endlich, so auch die Abbildungsmenge:

$$\# \text{Abb}(X, Y) = \#(Y^X) = (\#Y)^{(\#X)}$$

Explizite Konstruktion: Jede Abzählung  $\mu : \{1, \dots, n\} \xrightarrow{\sim} X$  beschert uns

$$Y^X \cong Y^n : f \mapsto (f(\mu(1)), \dots, f(\mu(n))).$$

**Beweis:** Die Bijektion  $Y^X \cong Y^n$  ist hier explizit angegeben. Damit können wir direkt den vorigen Satz E2E anwenden.

Für jede natürliche Zahl  $n \in \mathbb{N}_{\geq 0}$  haben wir die kanonische Bijektion

$$(\eta, \varepsilon) : \text{Abb}(\{1, \dots, n\}, Y) \cong Y^n.$$

Für  $f : \{1, \dots, n\} \rightarrow Y$  definieren wir  $\eta(f) := (f(1), \dots, f(n))$ .

Für  $y = (y_1, \dots, y_n) \in Y^n$  definieren wir  $\varepsilon(y) := f$  als die Abbildung  $f : \{1, \dots, n\} \rightarrow Y : 1 \mapsto y_1, \dots, n \mapsto y_n$ ; diese ist dadurch wohldefiniert.

Damit gilt  $\varepsilon \circ \eta = \text{id}$  und  $\eta \circ \varepsilon = \text{id}$ .

Gegeben sei eine Abzählung  $\mu : \{1, \dots, n\} \xrightarrow{\sim} X$ . Dann konstruieren wir

$$(\sigma, \tau) : \text{Abb}(X, Y) \cong \text{Abb}(\{1, \dots, n\}, Y).$$

Für  $f : X \rightarrow Y$  definieren wir  $\sigma(f) := f \circ \mu : \{1, \dots, n\} \rightarrow Y$ .

Für  $g : \{1, \dots, n\} \rightarrow Y$  definieren wir  $\tau(g) := g \circ \mu^{-1} : X \rightarrow Y$ .

Damit gilt  $\tau(\sigma(f)) = (f \circ \mu) \circ \mu^{-1} = f$ , also  $\tau \circ \sigma = \text{id}$ .

Ebenso gilt  $\sigma(\tau(g)) = (g \circ \mu^{-1}) \circ \mu = g$ , also  $\sigma \circ \tau = \text{id}$ .

Satz E2F nutzt die Komposition dieser beiden Bijektionen.

**Beispiel:** Über  $\{0, 1\}$  lassen sich vier 2-Tupel (Paare) bilden:

$$\{0, 1\}^2 = \{ (0, 0), (0, 1), (1, 0), (1, 1) \}$$

Ebenso können wir acht 3-Tupel (Tripel) bilden:

$$\{0, 1\}^3 = \{ (0, 0, 0), (0, 0, 1), (0, 1, 0), (0, 1, 1), \\ (1, 0, 0), (1, 0, 1), (1, 1, 0), (1, 1, 1) \}$$

Ebenso können wir sechzehn 4-Tupel (Quadrupel) bilden:

$$\{0, 1\}^4 = \{ (0, 0, 0, 0), (0, 0, 0, 1), (0, 0, 1, 0), (0, 0, 1, 1), \\ (0, 1, 0, 0), (0, 1, 0, 1), (0, 1, 1, 0), (0, 1, 1, 1), \\ (1, 0, 0, 0), (1, 0, 0, 1), (1, 0, 1, 0), (1, 0, 1, 1), \\ (1, 1, 0, 0), (1, 1, 0, 1), (1, 1, 1, 0), (1, 1, 1, 1) \}$$

Die Binärdarstellung definiert die Bijektion  $\{0, 1\}^n \cong \{0, \dots, 2^n - 1\}$ .

Die Potenzmenge  $\mathfrak{P}(X) = \{ A \subseteq X \}$  ist die Menge aller Teilmengen:

$$\mathfrak{P}(\emptyset) = \{ \emptyset \}$$

$$\mathfrak{P}(\{1\}) = \{ \emptyset, \{1\} \}$$

$$\mathfrak{P}(\{1, 2\}) = \{ \emptyset, \{1\}, \{2\}, \{1, 2\} \}$$

$$\mathfrak{P}(\{1, 2, 3\}) = \{ \emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\} \}$$

$$\mathfrak{P}(\{1, 2, 3, 4\}) = \{ \emptyset, \{1\}, \{2\}, \{3\}, \{4\},$$

$$\{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 3\}, \{2, 4\}, \{3, 4\},$$

$$\{1, 2, 3\}, \{1, 2, 4\}, \{1, 3, 4\}, \{2, 3, 4\}, \{1, 2, 3, 4\} \}$$

Jede Teilmenge  $A \subseteq \{1, 2, 3, 4\}$  entspricht einem Tupel  $f \in \{0, 1\}^4$ :

$$(0, 0, 0, 0) \leftrightarrow \{1, 2, 3, 4\}$$

$$(0, 1, 1, 0) \leftrightarrow \{1, 2, 3, 4\}$$

$$(1, 1, 1, 0) \leftrightarrow \{1, 2, 3, 4\}$$

$$(1, 1, 1, 1) \leftrightarrow \{1, 2, 3, 4\}$$

😊 Dieses Prinzip haben wir in Satz D3D allgemein ausgeführt.

## Satz E2G: Mächtigkeit der Potenzmenge

Für jede endliche Menge  $X$  mit  $n = \#X$  Elementen gilt:

$$\#\mathfrak{P}(X) = 2^n$$

Explizite Konstruktion: Satz D3D besichert uns die Bijektion

$$(\mathbf{I}, \text{supp}) : \mathfrak{P}(X) \cong \text{Abb}(X, \{0, 1\})$$

$$A \mapsto \mathbf{I}_A$$

$$\text{supp}(f) \leftarrow f$$

**Beweis:** Anschaulich ist der Satz plausibel, so wie oben illustriert, allzumal wenn es bloß um die vage „gefühlte Elementezahl“ geht.

Eine formale Abzählung gelingt mit der Bijektion aus Satz D3D, dank Satz E2F können wir die Mächtigkeit der Abbildungsmenge ablesen.

Da wir jeweils Bijektionen explizit angeben, erhalten wir auch hier durch Komposition eine explizite Bijektion  $\mathfrak{P}(X) \cong \{0, \dots, 2^n - 1\}$ . QED

**Aufgabe:** Wie viele Teilmengen hat die Menge  $X = \{0, 1, \dots, 9\}$ ?

**Lösung:** Die Menge  $X$  hat genau  $2^{10} = 1024$  verschiedene Teilmengen.

**Übung:** Konstruieren Sie, etwa im obigen Beispiel für  $n = 10$ , explizit eine Abzählung  $\mu : \{0, \dots, 2^n - 1\} \xrightarrow{\sim} \mathfrak{P}(\{0, \dots, n - 1\})$ .

**Aufgabe:** Wie viele Relationen gibt es zwischen  $X = \{1, 2, 3\}$  und  $Y = \{0, 1, \dots, 99\}$ ? Wie viele davon sind Funktionen?

**Lösung:** Relation bedeutet  $F \subseteq X \times Y$ , also  $F \in \mathfrak{P}(X \times Y)$ :

$$\#\mathfrak{P}(X \times Y) = 2^{3 \cdot 100} = 1024^{30} \approx 10^{90}$$

Funktion bedeutet zudem linkstotal und rechtseindeutig:

$$\#\text{Abb}(X, Y) = 100^3 = 10^6$$

😊 Relationen gibt es hier bereits astronomisch viele. Funktionen sind etwas besonderes und deutlich rarer.

Die Rechenregeln für Mengen sind wunderbar konkret und praktisch:

$$X \sqcup \emptyset = X = \emptyset \sqcup X, \quad X \cup \emptyset = X = \emptyset \cup X,$$

$$X \sqcup Y = Y \sqcup X, \quad X \cup Y = Y \cup X,$$

$$(X \sqcup Y) \sqcup Z = X \sqcup (Y \sqcup Z), \quad (X \cup Y) \cup Z = X \cup (Y \cup Z).$$

Das kartesische Produkt ist distributiv über die (disjunkte) Vereinigung:

$$X \times (Y \sqcup Z) = (X \times Y) \sqcup (X \times Z) \quad \text{ebenso für } \cup \text{ und } \cap$$

$$(X \sqcup Y) \times Z = (X \times Z) \sqcup (Y \times Z) \quad \text{ebenso für } \cup \text{ und } \cap$$

Für kartesische Produkte haben wir folgende kanonische Bijektionen:

$$X \times \{a\} \cong X \cong \{a\} \times X, \quad (x, a) \leftrightarrow x \leftrightarrow (a, x)$$

$$X \times Y \cong Y \times X, \quad (x, y) \leftrightarrow (y, x)$$

$$(X \times Y) \times Z \cong X \times (Y \times Z), \quad ((x, y), z) \leftrightarrow (x, (y, z))$$

Schließlich gelten die vertrauten Potenzgesetze:

$$Z^{(X \sqcup Y)} \cong Z^X \times Z^Y, \quad f \mapsto (f|_X, f|_Y)$$

$$(X \times Y)^Z \cong X^Z \times Y^Z, \quad f \mapsto (\text{pr}_1 \circ f, \text{pr}_2 \circ f)$$

😊 Die ersten acht Rechenregeln sind sofort klar, explizit und konkret.

Daraus folgen (erneut) die entsprechenden Rechenregeln für die natürlichen Zahlen. Der Nachweis per vollständiger Induktion ist länglich, die geometrische Realisierung ist dagegen anschaulich und konkret. Das nährt die Einsicht: Mengen sind konkret, Zahlen sind abstrakt.

Genauso wurde es Ihnen vermutlich in der Grundschule erklärt, ohne Bijektionen und Beweise. Jetzt verstehen Sie den Zusammenhang, Sie können nun Definitionen und Argumente präzise formulieren. So gesehen ist dies Schulmathematik vom höheren Standpunkt.

Die Bijektion  $Z^{(X \sqcup Y)} \cong Z^X \times Z^Y$  entsteht aus  $f \mapsto (f|_X, f|_Y)$  und umgekehrt  $(g, h) \mapsto f = g \sqcup h$ , also ausgeschrieben wie in Satz D2E:

$$f = g \sqcup h : X \sqcup Y \rightarrow Z : f(u) = \begin{cases} g(u) & \text{falls } u \in X, \\ h(u) & \text{falls } u \in Y. \end{cases}$$

Die Bijektion  $(X \times Y)^Z \cong X^Z \times Y^Z$  entsteht aus  $f \mapsto (\text{pr}_1 \circ f, \text{pr}_2 \circ f)$  und umgekehrt  $(g, h) \mapsto f$  mit  $f : Z \rightarrow X \times Y : f(x) = (g(x), h(x))$ .



## Satz E2H: Anzahl der Abbildungen, Injektionen und Bijektionen

Für je zwei Mengen  $X, Y$  mit  $\#X = k$  und  $\#Y = n$  gilt:

$$\# \text{Abb}(X, Y) = n^k$$

Die Anzahl der injektiven Abbildungen ist (dank Satz E1F):

$$\# \text{Inj}(X, Y) = n \cdot (n-1) \cdots (n-k+1) =: n^{\underline{k}}$$

Im Spezialfall  $k = n$  erhalten wir demnach

$$\# \text{Abb}(X, Y) = n^n$$

sowie die Anzahl der Bijektionen:

$$\# \text{Bij}(X, Y) = n \cdot (n-1) \cdots 3 \cdot 2 \cdot 1 = n^{\underline{n}} =: n!$$

Die symmetrische Gruppe  $S_n = \text{Aut}(\{1, \dots, n\})$  hat  $n!$  Elemente.

Anschaulich ist das plausibel. Die formale Abzählung gelingt mit E1F:

**Beweis:** Dank Sortierung zur Stufenform (E1F) haben wir die Bijektion  $\{1, \dots, n\} \times \{2, \dots, n\} \times \cdots \times \{k, \dots, n\} \xrightarrow{\sim} \text{Inj}(\{1, \dots, k\}, \{1, \dots, n\})$  mit der Zuordnung  $(i_1, i_2, \dots, i_k) \mapsto f = (1, i_1) \circ (2, i_2) \circ \cdots \circ (k, i_k) \circ \iota$ . Daraus erhalten wir wunderbar direkt und explizit die Anzahl! QED

Es ist oft lehrreich, neu definierte Objekte zu zählen. Dies zwingt dazu, die Definition genau zu verstehen und klärt so Missverständnisse auf. *Defendit numerus.* [Die Zahl gibt Schutz.] Juvenal (58–138 n.Chr.), *Satiren*

😊 Nochmal zur Betonung: Abzählung E1D verlangt eine Bijektion, also sollten wir eine möglichst konkrete Bijektion vorweisen können. Die Mengen  $\{1, \dots, n\}$  sind das Urmeter, der universelle Maßstab, mit dem wir die Größe einer beliebigen endlichen Menge messen.

😊 Die Nummerierung erlaubt direkten Zugriff auf alle Elemente. Sie wissen, wie viele es gibt, und sie können jedes adressieren. So generieren Sie eine gleichverteilt zufällige Injektion / Bijektion.

## Illustration zu Permutationen

Ich schreibe Permutationen kurz und bequem in Listennotation:

$$\left[ \begin{array}{c} 1 \ 2 \ \dots \ n \\ a_1 \ a_2 \ \dots \ a_n \end{array} \right] = [a_1, a_2, \dots, a_n]$$

Permutationen der Menge  $\{1, 2\}$ :

$$[1, 2], [2, 1]$$

Permutationen der Menge  $\{1, 2, 3\}$ :

$$[1, 2, 3], [1, 3, 2], [2, 1, 3], [2, 3, 1], [3, 1, 2], [3, 2, 1]$$

Permutationen der Menge  $\{1, 2, 3, 4\}$ :

$$\begin{aligned} & [1, 2, 3, 4], [1, 2, 4, 3], [1, 3, 2, 4], [1, 3, 4, 2], [1, 4, 2, 3], [1, 4, 3, 2], \\ & [2, 1, 3, 4], [2, 1, 4, 3], [2, 3, 1, 4], [2, 3, 4, 1], [2, 4, 1, 3], [2, 4, 3, 1], \\ & [3, 1, 2, 4], [3, 1, 4, 2], [3, 2, 1, 4], [3, 2, 4, 1], [3, 4, 1, 2], [3, 4, 2, 1], \\ & [4, 1, 2, 3], [4, 1, 3, 2], [4, 2, 1, 3], [4, 2, 3, 1], [4, 3, 1, 2], [4, 3, 2, 1] \end{aligned}$$

## Illustration zur Fakultät

Rekursionsformel:  $0! = 1$  und  $(n+1)! = n! \cdot (n+1)$ .

Ausgeschrieben:  $n! = 1 \cdot 2 \cdot 3 \cdots n$ . Die ersten Werte sind:

$0! = 1$	$7! = 5\,040$	$14! = 87\,178\,291\,200$
$1! = 1$	$8! = 40\,320$	$15! = 1\,307\,674\,368\,000$
$2! = 2$	$9! = 362\,880$	$16! = 20\,922\,789\,888\,000$
$3! = 6$	$10! = 3\,628\,800$	$17! = 355\,687\,428\,096\,000$
$4! = 24$	$11! = 39\,916\,800$	$18! = 6\,402\,373\,705\,728\,000$
$5! = 120$	$12! = 479\,001\,600$	$19! = 121\,645\,100\,408\,832\,000$
$6! = 720$	$13! = 6\,227\,020\,800$	$20! = 2\,432\,902\,008\,176\,640\,000$

Die **Stirling-Formel** bietet eine gute Näherung für große  $n$ :

$$n! \sim \sqrt{2\pi n} \left(\frac{n}{e}\right)^n$$

Diese Näherung werden Sie in der Analysis ausführlich behandeln, sowie viele weitere nützliche Approximationen und Grenzwerte.

Für  $z \in \mathbb{C}$  und  $k \in \mathbb{N}$  definieren wir den **Binomialkoeffizienten**

$$\binom{z}{k} := \frac{z(z-1)\cdots(z-k+1)}{k \cdot (k-1) \cdots 1} = \prod_{j=0}^{k-1} \frac{z-j}{k-j} = \frac{z^k}{k!}$$

Speziell für natürliche Zahlen  $n \in \mathbb{N}$  und  $0 \leq k \leq n$  gilt:

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \binom{n}{n-k}$$

Aus der Definition folgt sofort:

$$\binom{z+1}{k+1} = \binom{z}{k} \frac{z+1}{k+1} \quad \text{und} \quad \binom{z}{k+1} = \binom{z}{k} \frac{z-k}{k+1}$$

Daraus erhalten wir **Pascals Rekursionsformel**:

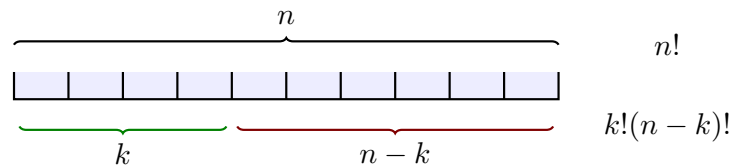
$$\binom{z+1}{k+1} = \binom{z}{k} + \binom{z}{k+1}$$

Hieraus erhalten wir das **Pascal-Dreieck für Binomialkoeffizienten**:

$\binom{n}{k}$	$k=0$	1	2	3	4	5	6	7	8	9	10
$n=0$	1										
1	1	1									
2	1	2	1								
3	1	3	3	1							
4	1	4	6	4	1						
5	1	5	10	10	5	1					
6	1	6	15	20	15	6	1				
7	1	7	21	35	35	21	7	1			
8	1	8	28	56	70	56	28	8	1		
9	1	9	36	84	126	126	84	36	9	1	
10	1	10	45	120	210	252	210	120	45	10	1

$$\binom{n+1}{k+1} = \binom{n}{k} + \binom{n}{k+1}$$

Auf wie viele Arten können wir aus  $n$  Objekten genau  $k$  auswählen?



Die Gesamtzahl der Möglichkeiten ist

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

**Kombinatorische Herleitung:** Wir können alle  $n$  Elemente auf  $n!$  Arten anordnen. Bei jeder Anordnung wählen wir die ersten  $k$  Elemente aus. Die ersten  $k$  Elemente dürfen wir dabei auf  $k!$  Arten beliebig umordnen. Die letzten  $n-k$  Elemente dürfen wir auf  $(n-k)!$  Arten umordnen. Die Auswahl ändert sich hierdurch nicht. Dies liefert die obige Formel.

**Aufgabe:** Zeigen Sie diese Aussage durch Induktion über  $n$ . Der folgende Beweis führt dies sorgsam aus.

**Satz E21:** Teilmengen und Binomialkoeffizient

Wir betrachten eine Menge  $X$  und ihre  $k$ -elementigen Teilmengen:

$$\binom{X}{k} = \mathfrak{P}_k(X) := \{ A \subseteq X \mid \#A = k \}$$

Ist  $X$  endlich, so auch  $\binom{X}{k}$ , und es gilt:

$$\#\binom{X}{k} = \binom{\#X}{k}$$

**Beweis:** Wir führen Induktion über die Anzahl  $n = \#X$  der Elemente. Der Induktionsanfang  $n = 0$  ist klar; sei also  $n \geq 1$ . Hier ist  $k = 0$  klar; sei also auch  $k \geq 1$ . Wir wählen  $z \in X$ . Für  $U = X \setminus \{z\}$  gilt dann:

$$\binom{X}{k} = \binom{U}{k} \sqcup \{ A \cup \{z\} \mid A \in \binom{U}{k-1} \} \cong \binom{U}{k} \sqcup \binom{U}{k-1}$$

Dank  $\#U = n-1$  können wir die Induktionsvoraussetzung anwenden:

$$\#\binom{X}{k} = \binom{n-1}{k} + \binom{n-1}{k-1} = \binom{n}{k}$$

**Beispiele:** Für je zwei reelle Zahlen  $a, b \in \mathbb{R}$  gilt:

$$(a + b)^0 = 1$$

$$(a + b)^1 = 1 \cdot a + 1 \cdot b$$

$$(a + b)^2 = 1 \cdot a^2 + 2 \cdot ab + 1 \cdot b^2$$

$$(a + b)^3 = 1 \cdot a^3 + 3 \cdot a^2b + 3 \cdot ab^2 + 1 \cdot b^3$$

$$(a + b)^4 = 1 \cdot a^4 + 4 \cdot a^3b + 6 \cdot a^2b^2 + 4 \cdot ab^3 + 1 \cdot b^4$$

$$(a + b)^5 = 1 \cdot a^5 + 5 \cdot a^4b + 10 \cdot a^3b^2 + 10 \cdot a^2b^3 + 5 \cdot a^1b^4 + 1 \cdot b^5$$

😊 Der Koeffizient vor  $a^k b^{n-k}$  ist genau der Binomialkoeffizient  $\binom{n}{k}$ .

Den ersten interessanten Fall  $n = 2$  kennen Sie als „erste binomische Formel“ aus der Schule. Diese nützliche Rechenregel gilt für alle  $n \in \mathbb{N}$ : Das ist die Aussage des binomischen Lehrsatzes. Er gilt in jedem Ring, sogar Halbring, solange die beiden Elemente kommutieren:  $ab = ba$ .

**Übung:** Beweisen Sie diesen Satz per Induktion über  $n$ . Dabei wird das Induktionsargument des vorigen Beweises auf Summen angewendet.

**Satz E2J: der binomische Lehrsatz**

Sei  $(R, +, \cdot)$  ein Halbring und  $a, b \in R$  mit  $ab = ba$ . Für alle  $n \in \mathbb{N}$  gilt:

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

**Beweis:** Wir sammeln alle Terme  $a^k b^{n-k}$  des  $n$ -fachen Produkts

$$(a + b)(a + b) \cdots (a + b).$$

Der Koeffizient vor dem Term  $a^k b^{n-k}$  ist die Anzahl  $\binom{n}{k}$ . □

😊 Speziell für  $a = b = 1$  in  $\mathbb{N}$  erhalten wir:

$$2^n = \sum_{k=0}^n \binom{n}{k} \quad \text{entsprechend} \quad \mathfrak{P}(\{1, \dots, n\}) = \bigsqcup_{k=0}^n \mathfrak{P}_k(\{1, \dots, n\})$$

Speziell für  $(a, b) = (p, 1 - p)$  in  $\mathbb{R}_{\geq 0}$  erhalten wir die Binomialverteilung

$$B(n, p)(k) = \binom{n}{k} p^k (1 - p)^{n-k} \quad \text{mit} \quad \sum_{k=0}^n B(n, p)(k) = 1.$$

Der binomische Lehrsatz E2J liefert uns algebraisch die Gleichung  $2^n = \sum_{k=0}^n \binom{n}{k}$  für alle  $n \in \mathbb{N}$ . Diese können wir konkret für Mengen realisieren und ablesen:  $\mathfrak{P}(\{1, \dots, n\}) = \bigsqcup_{k=0}^n \mathfrak{P}_k(\{1, \dots, n\})$ .

**Aufgabe:** (0) Erklären Sie die Symmetrie  $\binom{n}{k} = \binom{n}{n-k}$  der Binomialkoeffizienten durch eine geeignete Bijektion.

(1) Zeigen Sie die folgende **Vandermonde-Identität**, indem Sie sie durch geeignete Mengen konkret darstellen:

$$\sum_{k=0}^{\ell} \binom{m}{k} \binom{n}{\ell-k} = \binom{m+n}{\ell}, \quad \sum_{k=0}^n \binom{n}{k}^2 = \binom{2n}{n}$$

**Lösung:** (0) Sei  $X$  eine  $n$ -elementige Menge. Das Komplement  $\mathbb{C}: \mathfrak{P}(X) \rightarrow \mathfrak{P}(X): A \mapsto X \setminus A$  bildet  $k$ -elementige Teilmengen auf  $(n - k)$ -elementige Teilmengen ab. Dank  $\mathbb{C} \circ \mathbb{C} = \text{id}$  erhalten wir:

$$(\mathbb{C}, \mathbb{C}) : \binom{X}{k} \cong \binom{X}{n-k}$$

(1) Wir betrachten  $X = \{1, \dots, m\}$  und  $Y = \{m + 1, \dots, m + n\}$ . Für die  $\ell$ -elementigen Teilmengen von  $Z = X \sqcup Y$  gilt dann:

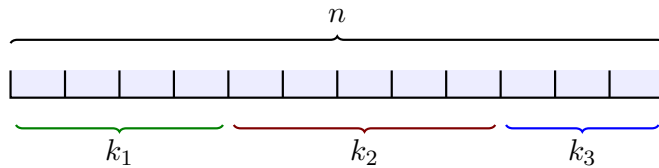
$$\binom{Z}{\ell} = \bigsqcup_{k=0}^{\ell} \left\{ A \sqcup B \mid A \in \binom{X}{k}, B \in \binom{Y}{\ell-k} \right\} \cong \bigsqcup_{k=0}^{\ell} \binom{X}{k} \times \binom{Y}{\ell-k}$$

Die Bijektion „ $\cong$ “ schickt  $C \in \binom{Z}{\ell}$  auf  $(C \cap X, C \cap Y) \in \binom{X}{k} \times \binom{Y}{\ell-k}$  und umgekehrt  $(A, B) \in \binom{X}{k} \times \binom{Y}{\ell-k}$  zurück auf  $A \sqcup B \in \binom{Z}{\ell}$ .

(2) Die zweite Gleichung folgt als Spezialfall für  $n = m = \ell$ . Hierbei nutzen wir  $\binom{n}{n-k} = \binom{n}{k}$ , siehe (0).

😊 In manchen Fällen sind Zahlen einfacher: Wir begnügen uns dann mit der Anzahl der Elemente und vernachlässigen die Menge selbst. In anderen Fällen ist die dahinterliegende Menge einfacher oder informativer, dann lohnt es sich, die reichere Struktur zu nutzen.

Auf wie viele Arten können wir  $n$  Objekte in  $\ell$  Mengen zu  $k_1, \dots, k_\ell$  Elementen aufteilen? Hierbei sei  $k_1, \dots, k_\ell \geq 0$  und  $k_1 + \dots + k_\ell = n$ .



Die Gesamtzahl der Möglichkeiten ist

$$\binom{n}{k_1, k_2, \dots, k_\ell} := \frac{n!}{k_1! \cdot k_2! \cdot \dots \cdot k_\ell!}$$

**Kombinatorische Herleitung:** Wir können alle  $n$  Elemente auf  $n!$  Arten anordnen. Die ersten  $k_1$  bilden die erste Menge, die nächsten  $k_2$  bilden die zweite Menge, usw. Innerhalb der  $i$ ten Menge können wir jeweils auf  $k_i!$  Arten beliebig umordnen. Dies liefert die obige Formel.

**Aufgabe:** Wie viele Kartenverteilungen gibt es beim Skat?

**Lösung:** Von 32 Karten bekommt jeder der drei Spieler 10 Karten:

$$\binom{32}{10, 10, 10, 2} = \frac{32!}{10! 10! 10! 2!} \approx 2.75 \cdot 10^{15}$$

**Aufgabe:** Auf wie viele Weisen lassen sich 12 (verschiedenfarbige) Bonbons gerecht unter zwei / drei / vier / zwölf Kindern aufteilen?

**Lösung:** Die Anzahl der möglichen Aufteilungen berechnen wir zu:

$$\begin{aligned} \binom{12}{6, 6} &= \frac{12!}{6! 6!} = 924 \\ \binom{12}{4, 4, 4} &= \frac{12!}{4! 4! 4!} = 34650 \\ \binom{12}{3, 3, 3, 3} &= \frac{12!}{3! 3! 3! 3!} = 369600 \\ \binom{12}{1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1} &= 12! = 479001600 \end{aligned}$$

**Aufgabe:** Wie wahrscheinlich ist es, bei 10 Münzwürfen genau 7 mal Kopf und 3 mal Zahl zu erhalten?

$$\begin{aligned} \Omega &= \{0, 1\}^{10}, & |\Omega| &= 2^{10} = 1024 \\ A &= \left\{ \begin{array}{l} \text{Ergebnisse } \omega \in \Omega \text{ mit} \\ \omega_1 + \dots + \omega_{10} = 3 \end{array} \right\}, & |A| &= \binom{10}{7, 3} = 120 \\ & & \mathbf{P}(A) &= |A|/|\Omega| \approx 0.117 \end{aligned}$$

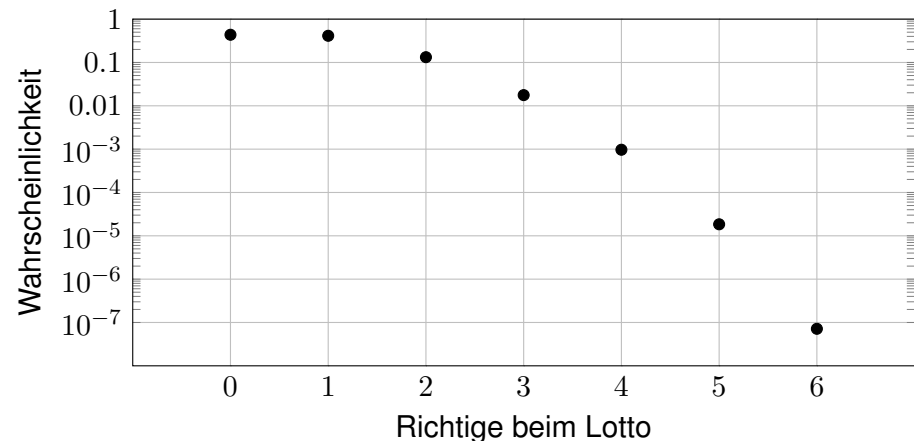
**Aufgabe:** Wie wahrscheinlich ist es, bei 10maligem Würfeln, die Augenzahlen 1, 2, 3, 4, 5, 6 mit Häufigkeit 1, 2, 3, 3, 0, 1 zu erhalten?

$$\begin{aligned} \Omega &= \{1, 2, 3, 4, 5, 6\}^{10}, & |\Omega| &= 6^{10} = 60\,466\,176 \\ A &= \left\{ \begin{array}{l} \text{Ergebnisse } \omega \in \Omega \text{ mit} \\ \text{diesen Häufigkeiten} \end{array} \right\}, & |A| &= \binom{10}{1, 2, 3, 3, 0, 1} = 50\,400 \\ & & \mathbf{P}(A) &= |A|/|\Omega| \approx 0.00083 \end{aligned}$$

**Aufgabe:** Mit welcher Wkt haben Sie  $k$  Richtige beim Lotto „6 aus 49“?

**Lösung:** Von  $N = 49$  Zahlen sind  $K = 6$  Treffer. Ein Tipp wählt  $n = 6$  der 49 Zahlen aus. Die Wkt für genau  $k$  Treffer ist demnach:

$$p(k) = H(N, K, n)(p) = \frac{\binom{K}{k} \binom{N-K}{n-k}}{\binom{N}{n}}$$



Eine **Zerlegung** von  $X$  ist ein Mengensystem  $Q \subseteq \mathfrak{P}(X)^*$  mit  $X = \bigsqcup Q$ .

**Beispiele:** Die Menge  $\{1\}$  erlaubt nur eine Zerlegung, nämlich  $\{\{1\}\}$ .

Die Menge  $\{1, 2\}$  erlaubt zwei Zerlegungen:  $\{\{1, 2\}\}$  und  $\{\{1\}, \{2\}\}$ .

Die Menge  $\{1, 2, 3\}$  erlaubt die folgenden fünf Zerlegungen:

$$\{\{1, 2, 3\}\}, \{\{1\}, \{2, 3\}\}, \{\{1, 2\}, \{3\}\}, \{\{1, 3\}, \{2\}\}, \{\{1\}, \{2\}, \{3\}\}.$$

Die Menge  $\{1, 2, 3, 4\}$  erlaubt die folgenden fünfzehn Zerlegungen:

$$\begin{aligned} &\{\{1, 2, 3, 4\}\}, \\ &\{\{1, 2\}, \{3, 4\}\}, \{\{1, 3\}, \{2, 4\}\}, \{\{1, 4\}, \{2, 3\}\}, \\ &\{\{1\}, \{2, 3, 4\}\}, \{\{2\}, \{1, 3, 4\}\}, \{\{3\}, \{1, 2, 4\}\}, \{\{4\}, \{1, 2, 3\}\}, \\ &\{\{1, 2\}, \{3\}, \{4\}\}, \{\{1, 3\}, \{2\}, \{4\}\}, \{\{1, 4\}, \{2\}, \{3\}\}, \\ &\{\{2, 3\}, \{1\}, \{4\}\}, \{\{2, 4\}, \{1\}, \{3\}\}, \{\{3, 4\}, \{1\}, \{2\}\}, \\ &\{\{1\}, \{2\}, \{3\}, \{4\}\}. \end{aligned}$$

Für Zerlegungen gibt es ein raffiniert rekursives Konstruktionsverfahren! Jede  $k$ -Zerlegung von  $\{1, \dots, n\}$  erhalten wir auf eine von zwei Arten:

- Wir nehmen eine  $(k - 1)$ -Zerlegung  $P$  von  $\{1, \dots, n - 1\}$  und fügen ihr die neue Klasse  $\{n\}$  hinzu: So erhalten wir  $Q = P \cup \{\{n\}\}$ .
- Wir nehmen eine  $k$ -Zerlegung  $P$  von  $\{1, \dots, n - 1\}$  und fügen einer Klasse  $C \in P$  das Element  $n$  hinzu:  $Q = (P \setminus \{C\}) \cup \{C \cup \{n\}\}$ .

**Übung:** Führen Sie dies für die 3-Zerlegungen von  $\{1, \dots, 4\}$  aus, zur Illustration ebenso für alle weiteren Zerlegungen von  $\{1, \dots, 4\}$ .

Wenn Sie Freude an dieser Rekursion haben, dann können Sie so systematisch alle Zerlegungen von  $\{1, \dots, 5\}$  konstruieren. Zur Kontrolle haben Sie die folgende Tabelle der Stirling-Zahlen.

Wenn Sie Freude an der Programmierung haben, dann können Sie diese Rekursion auch direkt in ein Computerprogramm umsetzen.

**Satz E2k:** Zerlegungen und Stirling-Zahlen

Wir betrachten eine Menge  $X$  und ihre  $k$ -elementigen Zerlegungen:

$$\left\{ \begin{matrix} X \\ k \end{matrix} \right\} := \left\{ Q \subseteq \mathfrak{P}(X)^* \mid X = \bigsqcup Q \text{ Zerlegung mit } \#Q = k \right\}$$

Ist  $X$  endlich mit  $\#X = n$ , so definieren wir die **Stirling-Zahl**

$$\left\{ \begin{matrix} n \\ k \end{matrix} \right\} := \# \left\{ \begin{matrix} X \\ k \end{matrix} \right\}.$$

Für  $n \geq 1$  gilt  $\left\{ \begin{matrix} n \\ 1 \end{matrix} \right\} = \left\{ \begin{matrix} n \\ n \end{matrix} \right\} = 1$  sowie  $\left\{ \begin{matrix} n \\ 0 \end{matrix} \right\} = \left\{ \begin{matrix} n \\ k \end{matrix} \right\} = 0$  für alle  $k > n$ .

Die weiteren Werte erhalten wir dank folgender Rekursionsformel:

$$\left\{ \begin{matrix} n \\ k \end{matrix} \right\} = \left\{ \begin{matrix} n - 1 \\ k - 1 \end{matrix} \right\} + k \left\{ \begin{matrix} n - 1 \\ k \end{matrix} \right\}$$

**Beweis:** Für  $\#X = n \geq 1$  wählen wir  $z \in X$  und setzen  $U = X \setminus \{z\}$ :

$$\left\{ \begin{matrix} X \\ k \end{matrix} \right\} = \left\{ Q \in \left\{ \begin{matrix} X \\ k \end{matrix} \right\} \mid \{z\} \in Q \right\} \sqcup \left\{ Q \in \left\{ \begin{matrix} X \\ k \end{matrix} \right\} \mid \{z\} \notin Q \right\} \cong \left\{ \begin{matrix} U \\ k - 1 \end{matrix} \right\} \sqcup k \left\{ \begin{matrix} U \\ k \end{matrix} \right\}$$

Die abkürzende Schreibweise dieser Bijektion bedarf der Erläuterung.

Die Bezeichnung „ $k \left\{ \begin{matrix} U \\ k \end{matrix} \right\}$ “ ist leider etwas verwickelt: Wir nehmen eine  $k$ -Zerlegung  $P$  von  $U$ , fügen einer Klasse  $C \in P$  das Element  $z$  hinzu und erhalten  $Q = (P \setminus \{C\}) \cup \{C \cup \{z\}\}$ . Hierbei haben wir  $k$  mögliche Wahlen von  $C$ . Die hierzu benötigten Daten sind daher:

$$k \left\{ \begin{matrix} U \\ k \end{matrix} \right\} := \left\{ (P, C) \mid C \in P \in \left\{ \begin{matrix} U \\ k \end{matrix} \right\} \right\}$$

Wir betrachten also Zerlegungen  $P$  mit einer markierten Klasse  $C \in P$ . Jede  $k$ -Zerlegung  $P$  erlaubt  $k$  Markierungen  $C \in P$ . Hierzu gehört die Abbildung  $k \left\{ \begin{matrix} U \\ k \end{matrix} \right\} \rightarrow \left\{ \begin{matrix} U \\ k \end{matrix} \right\} : (P, C) \mapsto P$ . Über jeder Zerlegung  $P$  liegen die  $k$  möglichen Wahlen  $(P, C)$  als Elemente der Faser. Wir erhalten somit

$$\left\{ \begin{matrix} X \\ k \end{matrix} \right\} \cong \left\{ \begin{matrix} U \\ k - 1 \end{matrix} \right\} \sqcup k \left\{ \begin{matrix} U \\ k \end{matrix} \right\}$$

wie gewünscht mit der Elementezahl  $\#k \left\{ \begin{matrix} U \\ k \end{matrix} \right\} = k \cdot \# \left\{ \begin{matrix} U \\ k \end{matrix} \right\}$ .

**Übung:** Schreiben Sie diese Bijektion nun explizit aus.

Hieraus erhalten wir das **Stirling–Dreieck für Zerlegungszahlen**:

$\left\{ \begin{matrix} n \\ k \end{matrix} \right\}$	k=1	2	3	4	5	6	7	8	9	10
n=1	1									
2	1	1								
3	1	3	1							
4	1	7	6	1						
5	1	15	25	10	1					
6	1	31	90	65	15	1				
7	1	63	301	350	140	21	1			
8	1	127	966	1701	1050	266	28	1		
9	1	255	3025	7770	6951	2646	462	36	1	
10	1	511	9330	34105	42525	22827	5880	750	45	1

$$\left\{ \begin{matrix} n \\ k \end{matrix} \right\} = \left\{ \begin{matrix} n-1 \\ k-1 \end{matrix} \right\} + k \left\{ \begin{matrix} n-1 \\ k \end{matrix} \right\}$$

Diese Werte heißen **Stirling–Zahlen zweiter Art**. Es gibt daneben auch die Stirling–Zahlen erster Art, die wir hier nicht betrachten.

😊 Die ersten vier Zeilen entsprechen den Anzahlen der Zerlegungen, die wir eingangs auf Seite E241 explizit ausgeschrieben haben. Wenn Sie nun alle Zerlegungen von  $\{1, 2, 3, 4, 5\}$  auflisten möchten, dann können Sie zumindest deren Anzahl mit der Tabelle prüfen.

😊 Die erste Spalte  $\left\{ \begin{matrix} n \\ 1 \end{matrix} \right\} = 1$  und die Diagonale  $\left\{ \begin{matrix} n \\ n \end{matrix} \right\} = 1$  sind klar: Für jede  $n$ -elementige Menge  $X = \{x_1, \dots, x_n\}$  haben wir genau eine 1-Zerlegung, nämlich  $\{\{x_1, \dots, x_n\}\}$ , und genau eine  $n$ -Zerlegung, nämlich  $\{\{x_1\}, \dots, \{x_n\}\}$ . Das ist bei der Rekursion hilfreich.

😊 Die erste Nebendiagonale  $\left\{ \begin{matrix} n \\ n-1 \end{matrix} \right\} = \binom{n}{2}$  ist leicht zu verstehen: Wir zerlegen  $X$  in  $n - 1$  Klassen, gemäß  $\{\{x_1, x_2\}, \{x_3\}, \dots, \{x_n\}\}$ . Das bedeutet, genau zwei Elemente liegen in einer gemeinsamen Klasse, alle anderen Elemente sind jeweils allein in ihrer Klasse.

😊 In der zweiten Spalte gilt  $\left\{ \begin{matrix} n \\ 2 \end{matrix} \right\} = (2^n - 2)/2 = 2^{n-1} - 1$ : Jede Zerlegung  $\{A, B\}$  entspricht  $A \in \mathfrak{P}(X) \setminus \{\emptyset, X\}$  und  $B = X \setminus A$ . Die weiteren Zerlegungszahlen sind nicht so einfach zu erklären. Zum Glück haben wir die obige Rekursion, damit gelingt es!

😊 Für die Binomialkoeffizienten haben wir eine geschlossene Formel:

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

Daraus haben wir Pascals Rekursionsformel abgeleitet und Pascals Dreieck erhalten. Sie nützt ebenso in zahlreichen weiteren Rechnungen und wird Ihnen auch in den Übungen immer wieder begegnen.

Für die Stirling–Zahlen  $\left\{ \begin{matrix} n \\ k \end{matrix} \right\}$  hingegen haben wir keine ebenso schöne, geschlossene Formel, sondern nur die Rekursionsformel aus Satz E2k. Das genügt immerhin für unsere ersten Rechnungen und Beispiele. Die kleinen Werte haben wir im Stirling–Dreieck tabelliert.

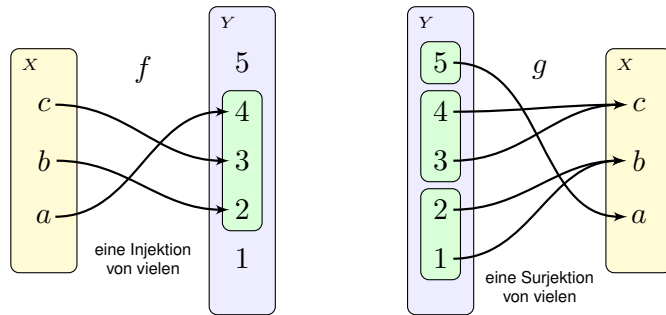
Binomialkoeffizienten und Stirling–Zahlen und weitere kombinatorische Koeffizienten kommen in vielen, sehr unterschiedlichen Kontexten vor. Daher gibt es eine ausgedehnte Literatur zu nützlichen Formeln, Identitäten und Näherungen. Das ist beruhigend zu wissen.

😊 Die Rekursion gilt nicht nur für die Anzahlen, auch für die Mengen! Sie können so alle Zerlegungen explizit generieren. Solche konkreten Konstruktionen sind eine wunderbare Programmierübung. Mehr dazu finden Sie im monumentalen Werk von Donald E. Knuth: *The Art of Computer Programming*, vol. 4A, §7.2.1.5 Generating all set partitions.

Wenn Sie sich ernsthaft für die Programmierung und langfristig auch für effiziente Algorithmen interessieren, dann sollten Sie unbedingt diese Bibel der Programmierkunst konsultieren. Keine leichte Kost, sondern ein nie versiegender Quell nahrhafter Erkenntnis.

*Fun fact:* Für seine TAOCP-Bücher erschuf Knuth das Textsatzsystem  $\text{T}_{\text{E}}\text{X}$ , mit dem heute alle Welt (natur)wissenschaftliche Texte schreibt, und mit dem auch dieses Dokument für Sie erstellt wurde.

Als kleines Beispiel zur Illustration betrachten wir eine 3-elementige Menge  $X = \{a, b, c\}$  und eine 5-elementige Menge  $Y = \{1, 2, 3, 4, 5\}$ .



**Aufgabe:**

- (1) Wie viele Injektionen  $f : \{a, b, c\} \hookrightarrow \{1, 2, 3, 4, 5\}$  gibt es?
- (2) Wie viele Surjektionen  $g : \{1, 2, 3, 4, 5\} \twoheadrightarrow \{a, b, c\}$  gibt es?

**Lösung:**

- (1) Es gibt genau  $\binom{5}{3} \cdot 3! = 10 \cdot 6 = 60$  Injektionen.
- (2) Es gibt genau  $\binom{5}{3} \cdot 3! = 25 \cdot 6 = 150$  Surjektionen.

☺ Das ist eine erste Anwendung der **kanonischen Faktorisierung**. Die Aufteilung in kleinere, leichtere Teilprobleme ist allgemein nützlich.

**Satz E2L: Anzahl der Injektionen und der Surjektionen**

Für alle endlichen Mengen  $X, Y$  mit  $\#X = k$  und  $\#Y = n$  gilt:

$$\# \text{Inj}(X, Y) = \#\{ f : X \hookrightarrow Y \} = \binom{n}{k} \cdot k!$$

$$\# \text{Sur}(Y, X) = \#\{ f : Y \twoheadrightarrow X \} = \left\{ \begin{matrix} n \\ k \end{matrix} \right\} \cdot k!$$

Im Spezialfall  $k = n$  erhalten wir erneut  $\# \text{Bij}(X, Y) = \# \text{Bij}(Y, X) = k!$ .

**Beweis:** (1) Wir haben  $\binom{n}{k}$  Wahlen der Bildmenge  $B \in \binom{Y}{k}$ . Zu gegebenem  $B$  haben wir dann  $k!$  Zuordnungen  $X \xrightarrow{\sim} B$ .

(2) Wir haben  $\left\{ \begin{matrix} n \\ k \end{matrix} \right\}$  Wahlen der Zerlegung  $Q \in \{Y\}_k$  in Fasern. Zu gegebenem  $Q$  haben wir dann  $k!$  Zuordnungen  $Q \xrightarrow{\sim} X$ . ◻

Ich führe hier die zweite Konstruktion (2) noch etwas genauer aus. Die nachfolgende Aufgabe zeigt ein einfaches, konkretes Beispiel. Jede surjektive Abbildung  $f : Y \twoheadrightarrow X$  definiert eine Zerlegung in Fasern:

$$Q = \{ f^{-1}(\{x\}) \subseteq Y \mid x \in X \} \subseteq \mathfrak{P}(Y)^*, \quad \bigsqcup Q = Y.$$

Hat  $X$  genau  $k$  Elemente, so erhalten wir eine Zerlegung mit  $\#Q = k$ .

Umgekehrt können wir aus einer Zerlegung  $Q$  in  $k = \#Q$  Klassen eine Surjektion  $f : Y \twoheadrightarrow X$  konstruieren, indem wir jede Klasse  $C \in Q$  auf ein Element  $x \in X$  abbilden. Hierzu gibt es genau  $k!$  Möglichkeiten.

Warum? Damit  $f : Y \twoheadrightarrow X$  surjektiv wird, muss auch die Zuordnung  $f' : Q \rightarrow X$  surjektiv sein. Wegen  $\#Q = \#X = k$  ist  $f'$  somit auch injektiv, also insgesamt bijektiv, kurz  $f' : Q \xrightarrow{\sim} X$  (siehe Satz E1H).

☺ Unsere Werkzeuge ermöglichen das strukturierte Abzählen! Ohne die abstrakte Methode sind die konkreten Zahlenbeispiele kaum zu lösen; mit dem passenden Satz an Werkzeugen ist es jedoch leicht.

**Aufgabe:** Als konkretes Beispiel sei  $Y = \{1, 2, 3, 4\}$  und  $X = \{a, b\}$ .

- (1) Nennen Sie alle Zerlegungen  $Q$  von  $Y$  in zwei Klassen.
- (2) Nennen Sie alle Surjektionen  $Y \twoheadrightarrow X$ . Bestimmen Sie zuerst (a) die Anzahlen und dann (b) die Objekte selbst.

**Lösung:** (1a) Dank Stirling-Dreieck finden wir die Anzahl  $\left\{ \begin{matrix} 4 \\ 2 \end{matrix} \right\} = 7$ .

(1b) Die sieben Zerlegungen der Menge  $Y$  in zwei Klassen sind:

$$\begin{aligned} & \{\{1, 2\}, \{3, 4\}\}, \{\{1, 3\}, \{2, 4\}\}, \{\{1, 4\}, \{2, 3\}\}, \\ & \{\{1\}, \{2, 3, 4\}\}, \{\{2\}, \{1, 3, 4\}\}, \{\{3\}, \{1, 2, 4\}\}, \{\{4\}, \{1, 2, 3\}\}, \end{aligned}$$

(2a) Wir erhalten  $2! \left\{ \begin{matrix} 4 \\ 2 \end{matrix} \right\} = 2 \cdot 7 = 14$  Surjektionen  $Y \twoheadrightarrow X$ .

(2b) Zu jeder Zerlegung  $Q = \{A, B\}$  der Startmenge  $Y$  gehören genau zwei Surjektionen  $f, g : Y \twoheadrightarrow X$  auf die Zielmenge  $X$ :

- eine erste mit  $f^{-1}(\{a\}) = A$  und  $f^{-1}(\{b\}) = B$ ,
- eine zweite mit  $g^{-1}(\{a\}) = B$  und  $g^{-1}(\{b\}) = A$ .

☺ Damit können wir alle vierzehn Surjektionen explizit ausschreiben.

**Aufgabe:** (Aus dem Mathekalender 2012) Sie backen  $k = 100$  Kekse. Sie geben  $n$  Chocolate Chips zum Teig, verteilen diese gründlich zufällig und teilen dann den Teig in 100 Kekse. Wieviele Chips brauchen Sie, damit mit 90% Sicherheit jeder Keks mindestens einen Chip enthält?

**Lösung:** Die Wkt, dass kein Chip im  $i$ ten Keks landet, ist  $(99/100)^n$ . Das Gegenereignis  $A_i = \{\text{In Keks } i \text{ ist mindestens ein Chip.}\}$  hat demnach die komplementäre Wahrscheinlichkeit  $\mathbf{P}(A_i) = 1 - 0.99^n$ .

(1) Näherung: Zur Vereinfachung rechnen wir zunächst, als wären die Ereignisse  $A_i$  unabhängig. (Das ist genau genommen nicht richtig, erweist sich anschließend aber als erstaunlich gute Näherung.)

Die gewünschte Bedingung vereinfacht sich dann zu:

$$f(n) := (1 - 0.99^n)^{100} \stackrel{!}{\geq} 0.9$$

Wir erhalten somit (mit Hilfe eines Taschenrechners):

$$n \geq \frac{\ln(1 - 0.9^{1/100})}{\ln 0.99} \approx 682.17$$

(2) Exakt gibt es  $k^n = 100^n$  Verteilungen der  $n$  Chips auf  $k = 100$  Kekse. Darunter sind genau  $k! \binom{n}{k}$  mit mindestens einem Chip in jedem Keks.

Anders gesagt: Es gibt  $k^n$  Abbildungen  $f: \{1, \dots, n\} \rightarrow \{1, \dots, k\}$ , davon sind genau  $k! \binom{n}{k}$  surjektiv. Ein Hoch auf Satz E2L!

Die gewünschte Bedingung ist demnach:

$$g(n) := \frac{k!}{k^n} \binom{n}{k} \stackrel{!}{\geq} 0.9$$

Ausrechnen für  $n = 100, 101, 102, \dots$  mit Hilfe eines Computers liefert:

$$g(682) = 0.899499\dots, \quad g(683) = 0.900455\dots$$

😊 Sie brauchen also tatsächlich 683 Chocolate Chips! Das rechtfertigt nachträglich die naive Näherung in der vereinfachten Rechnung (1).

Das erklärt noch nicht, warum diese Näherung so gut funktioniert, oder in welchen anderen Situationen Sie diesen Trick anwenden können. Hierzu ist zudem eine allgemeine Fehlerabschätzung notwendig.

**Aufgabe:** (1) Wie viele Abbildungen  $f: \{1, 2, 3, 4, 5\} \rightarrow \{1, 2, 3\}$  treffen genau zwei Bildpunkte, erfüllen also  $\# \text{im}(f) = 2$ ?

(2) Was gilt allgemein? Bestimmen Sie die Anzahl der Abbildungen  $f: X = \{1, \dots, k\} \rightarrow Y = \{1, \dots, n\}$  vom Rang  $r = \# \text{im}(f)$ .

**Lösung:** (2) Seien  $X, Y$  endliche Mengen mit  $\#X = k$  und  $\#Y = n$  sowie

$$\begin{aligned} \text{Abb}(X, Y)_r &:= \{ f: X \rightarrow Y \mid \# \text{im}(f) = r \} \\ &\cong \{ (Q, \bar{f}, B) \mid Q \in \binom{X}{r}, B \in \binom{Y}{r}, \bar{f}: Q \xrightarrow{\sim} B \}. \end{aligned}$$

Jede Abbildung  $f: X \rightarrow Y$  mit  $\# \text{im}(f) = r$  ist eindeutig bestimmt durch ihre Zerlegung  $Q \in \binom{X}{r}$  in Fasern und ihre Bildmenge  $B \in \binom{Y}{r}$  sowie die induzierte Bijektion  $\bar{f}: Q \xrightarrow{\sim} B$  zwischen beiden. Wir haben also:

$$\# \text{Abb}(X, Y)_r = \sum_{Q \in \binom{X}{r}} \sum_{B \in \binom{Y}{r}} \# \text{Bij}(Q, B) = \binom{k}{r} \cdot \binom{n}{r} \cdot r!$$

(1) Für  $(k, n, r) = (5, 3, 2)$  finden wir  $\binom{5}{2} = 15$  und  $\binom{3}{2} = 3$  und  $2! = 2$ , also insgesamt  $\# \text{Abb}(\{1, 2, 3, 4, 5\}, \{1, 2, 3\})_2 = 15 \cdot 3 \cdot 2 = 90$ .

Zusammenfassend erhalten wir den folgenden schönen Satz:

**Satz E2M: Anzahl der Abbildungen mit vorgegebenem Rang**

Seien  $X, Y$  endliche Mengen mit  $\#X = k$  und  $\#Y = n$  Elementen sowie

$$\text{Abb}(X, Y)_r := \{ f: X \rightarrow Y \mid \# \text{im}(f) = r \}.$$

Für jeden Rang  $r \in \mathbb{N}$  haben wir:

$$\# \text{Abb}(X, Y)_r = \binom{k}{r} \cdot \binom{n}{r} \cdot r!$$

Im Spezialfall  $r = k$  erhalten wir  $\# \text{Inj}(X, Y) = \binom{n}{r} \cdot r!$ .

Im Spezialfall  $r = n$  erhalten wir  $\# \text{Sur}(X, Y) = \binom{k}{r} \cdot r!$ .

Im Spezialfall  $r = k = n$  erhalten wir  $\# \text{Bij}(X, Y) = r!$ .

**Beweis:** Wir strukturieren die Menge  $\text{Abb}(X, Y)_r$  wie in der vorigen Aufgabe ausgeführt und gewinnen daraus die ersehnte Abzählung.  $\square$

😊 Diese allgemeine Technik perfektionieren wir durch die kanonische Faktorisierung E3I in Quotient-Bijektion-Inklusion  $X \twoheadrightarrow Q \xrightarrow{\sim} B \hookrightarrow Y$ .



**Beispiel:** Sei  $X = \{1, 2, 3, 4, 5, 6, 7\}$  und  $Q = \{\{1, 4\}, \{2, 3, 6, 7\}, \{5\}\}$ .

### Definition E3A: Zerlegung und Quotient

Sei  $X$  eine Menge. Eine **Zerlegung**  $Q$  von  $X$  ist ein Mengensystem  $Q \subseteq \mathfrak{P}(X)^*$  mit  $X = \bigsqcup Q$ . Explizit ausgeschrieben bedeutet das:

$$\bigcup Q = X \quad \wedge \quad \forall A, B \in Q : A = B \vee A \cap B = \emptyset$$

Jedes Element  $C \in Q$  nennen wir eine **Klasse** von  $Q$ , oft auch **Äquivalenzklasse**, je nach Kontext auch **Bahn** oder **Orbit**.

Jedes Element  $x \in X$  liegt demnach in genau einer Klasse  $C \in Q$ . Jedem Element  $x \in X$  ordnen wir seine Klasse  $C \in Q$  zu:

$$q : X \rightarrow Q : x \mapsto C \quad \text{mit} \quad x \in C \in Q$$

Übliche Schreibweisen sind  $q(x) = \text{cl}_Q(x) = [x]_Q = [x] = \bar{x} = \dots$

Die Zerlegung  $Q$  nennen wir auch eine **Quotientenmenge** von  $X$  und  $q : X \rightarrow Q$  die zugehörige **Quotientenabbildung**, kurz **Quotient**.

Jedes Element  $C \in Q$  nennen wir eine **Klasse** von  $Q$ , je nach Kontext auch **Äquivalenzklasse**, speziell bei Gruppenoperation auch **Bahn** oder **Orbit**; das sind alles schöne Namen für immer dieselbe Idee: eine Zerlegung von  $X$  in nicht-leere disjunkte Teilmengen.

Jedes Element  $x \in X$  liegt demnach in genau einer Klasse  $C \in Q$ .

Dies definiert die Zuordnung  $q : X \rightarrow Q : x \mapsto C$  mit  $x \in C \in Q$ .

Die Faser über dem Punkt  $C$  ist die Menge  $C$ , denn  $q^{-1}(\{C\}) = C$ .

Man nennt die Abbildung  $q$  daher auch die **kanonische Surjektion**.

Die Quotientenmenge  $Q$  und die Quotientenabbildung  $q : X \rightarrow Q$  nennt man beide auch kurz **Quotient**, wenn dabei klar wird, was gemeint ist. Diese auch so „abstrakte“ Konstruktion ist im Grunde konkret und explizit, einfach und elegant. Sie hat zahllose Anwendungen und Auswirkungen.

Daher ist es für Sie ganz sicher hilfreich, sich frühzeitig und gründlich damit vertraut zu machen. Ergreifen Sie also diese gute Gelegenheit. Mit etwas Gewöhnung verliert auch dieser neue Begriff schnell seinen Schrecken und wird auch für Sie zu einem vielseitigen Werkzeug.

**Beispiel:** Sei  $X = \{1, 2, 3, 4, 5, 6, 7\}$  und  $Q = \{\{1, 4\}, \{2, 3, 6, 7\}, \{5\}\}$ . Zu  $Q$  ist  $R = \{4, 3, 5\}$  ein Repräsentantensystem, ebenso  $\{1, 2, 5\}, \dots$

### Definition E3B: Repräsentantensystem

Eine Teilmenge  $R \subseteq X$  heißt **Repräsentantensystem** zu  $Q$ , falls gilt:

$$\forall C \in Q \quad \exists! x \in R : x \in C$$

Somit wählt  $R$  aus jeder Klasse  $C \in Q$  genau einen Repräsentanten. Die Einschränkung  $q|_R : R \rightarrow Q : x \mapsto [x]$  ist bijektiv. Die Umkehrung

$$r = q|_R^{-1} : Q \rightarrow X : C \mapsto r(C) \in C$$

ordnet jeder Klasse  $C \in Q$  ein Element  $r(C) \in C$  als Repräsentant zu.

**Beispiel:** Die Surjektion  $f : \mathbb{R} \rightarrow \mathbb{R}_{\geq 0} : x \mapsto y = x^2$  zerlegt  $\mathbb{R}$  in Fasern:

$$\mathbb{R} = \bigsqcup_{y \in \mathbb{R}_{\geq 0}} f^{-1}(\{y\})$$

Zur Klasse  $C = \{-x, x\}$  wählen wir den nicht-negativen Repräsentanten  $|x| \in C$ ; diese Wahlen definieren die Wurzelfunktion  $\sqrt{\cdot} : \mathbb{R}_{\geq 0} \rightarrow \mathbb{R}$ .

**Beispiel:** Die Menge  $M = \bigsqcup \{A_1, \dots, A_n\}$  der SchülerInnen teilt sich in Klassen auf und  $R = \{a_1, \dots, a_n\}$  enthält die KlassensprecherInnen. Die Abbildung  $r : A_i \mapsto a_i$  weist jeder Klasse ihren Repräsentanten zu. Die Wahl ist willkürlich; aus mathematischer Sicht sind alle gleich gut.

**Beispiel:** In  $(\mathbb{N}, \leq)$  hat jede nicht-leere Teilmenge  $A \subseteq \mathbb{N}$  ein kleinstes Element; wir können daher  $a = \min A$  als Repräsentanten wählen. Das ist zwar ebenso willkürlich, aber immerhin kanonisch, einheitlich. Oft sind wir froh, wenn uns die Qual der Wahl abgenommen wird.

☹ Meist ist die Wahl eines Repräsentantensystems ein Akt der Willkür. Zur Frage der Existenz siehe das Auswahlaxiom auf Seite D123.

☺ In günstigen Fällen kommen wir ohne willkürliche Wahlen aus. Man spricht dann auch von einer „natürlichen“ Konstruktion.

Meist liegt das daran, dass es nur eine Wahlmöglichkeit gibt, oder unter den vielen nur eine im Kontext „vernünftige“ und „richtige“ Wahl, zum Beispiel die kanonische, natürliche Bijektion in Satz D3D

## Die Klassengleichung: doppeltes Abzählen

E305

**Beispiel:** Für  $X = \{1, 2, 3, 4, 5, 6, 7\}$  und  $Q = \{\{1, 4\}, \{2, 3, 6, 7\}, \{5\}\}$  ist die Elementezahl  $\#X = 7$  gleich  $\sum_{C \in Q} \#C = 2 + 4 + 1$  gemäß  $Q$ .

### Lemma E3c: die Klassengleichung

Sei  $Q$  eine Zerlegung von  $X$ . Ist  $X$  endlich, so auch  $Q$  und

$$Q_n = \{C \in Q \mid \#C = n\} \quad \text{für jedes } n \in \mathbb{N}.$$

Damit gilt  $Q = \bigsqcup_{n \in \mathbb{N}} Q_n$ . Daraus folgt die **Klassengleichung**:

$$\#X = \sum_{C \in Q} \#C = \sum_{n \in \mathbb{N}} n \cdot \#Q_n,$$

also  $\#X = 1 \cdot \#Q_1 + 2 \cdot \#Q_2 + \dots + N \cdot \#Q_N$ , falls  $\#C \leq N$  für alle  $C \in Q$ .

Spezialfall: Haben alle Klassen  $C \in Q$  dieselbe Größe  $c = \#C$ , so gilt

$$\#X = c \cdot \#Q, \quad \text{also} \quad \#Q = (\#X)/c.$$

Der Tourist fragt den Schäfer: „Wie zählen Sie so schnell Ihre Schafe?“  
— „Das ist ganz einfach: Ich zähle die Beine und teile durch vier.“

## Die Klassengleichung: doppeltes Abzählen

E306  
Erläuterung

Wir haben  $Q = \bigsqcup_{n \in \mathbb{N}} Q_n$ . Doppeltes Abzählen ergibt demnach:

$$\#X = \sum_{C \in Q} \#C = \sum_{n \in \mathbb{N}} \sum_{C \in Q_n} \#C = \sum_{n \in \mathbb{N}} \sum_{C \in Q_n} n = \sum_{n \in \mathbb{N}} n \cdot \#Q_n$$

Haben alle Klassen  $C \in Q$  dieselbe Größe  $c = \#C$ , so gilt

$$\#X = c \cdot \#Q, \quad \text{also} \quad \#Q = (\#X)/c.$$

Die rechte Gleichung motiviert für  $Q$  den Namen **Quotientenmenge** von  $X$ . Manche schauen lieber auf die linke Gleichung und nennen  $Q$  dann konsequenterweise eine **Faktormenge** von  $X$ . Das ist dieselbe Sache, von zwei verschiedenen Seiten betrachten.

**Beispiel:** Die Menge  $X$  der Schüler einer Schule können Sie alle einzeln abzählen, oder erst klassenweise zählen und dann addieren. Das wird besonders einfach, wenn alle Klassen dieselbe Größe haben!

**Beispiel:** Einen Haufen Münzgeld können Sie unsortiert zählen, oder zuerst die 1-Cent-Münzen zusammenfassen, dann die 2-Cent-Münzen, die 5-Cent-Münzen, usw. Genau dasselbe tut die Klassengleichung

## Erstes Beispiel zur Klassengleichung

E307

Kontakt-Los-Generator: Auf wie viele Arten können wir  $n$  Studierende aufteilen in genau  $\ell$  Gruppen mit fester Größe  $k_1, \dots, k_\ell$ ?

$$\#X = n$$

1	2	3	4	5	6	7	8	9	10	11	12
5	7	1	4	11	12	6	3	9	10	8	2

$\underbrace{\hspace{10em}}_{\#X_1 = k_1} \quad \underbrace{\hspace{10em}}_{\#X_2 = k_2} \quad \underbrace{\hspace{10em}}_{\#X_3 = k_3}$

Wir fixieren  $X = \{1, \dots, n\} = X_1 \sqcup \dots \sqcup X_\ell$  mit  $\#X_i = k_i$  und nutzen

$$f : S_n \rightarrow \mathfrak{P}(X)^\ell : \sigma \mapsto (\sigma(X_1), \dots, \sigma(X_\ell)).$$

Jede Permutation  $\sigma \in S_n$  definiert eine Aufteilung  $f(\sigma)$ , wie gewünscht.

Alle Elemente ihrer Faser  $[\sigma] = f^{-1}(\{f(\sigma)\})$  liefern genau dasselbe.

Es gilt  $[\text{id}] = \{\sigma_1 \dots \sigma_\ell \mid \sigma_i \in S_{X_i}\} \cong S_{X_1} \times \dots \times S_{X_\ell}$  und  $\sigma : [\text{id}] \cong [\sigma]$ .

Jede solche Klasse  $[\sigma]$  hat die Mächtigkeit  $c = \#[\sigma] = k_1! k_2! \dots k_\ell!$ .

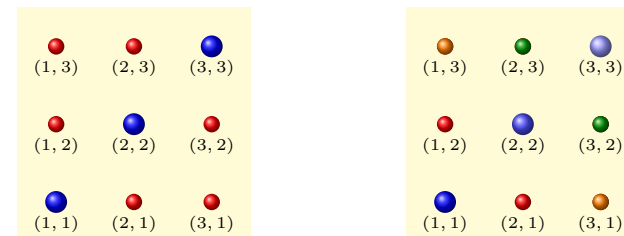
Wie viele Klassen gibt es? Klassengleichung  $\#S_n = n! = c \cdot \#Q$ .

😊 Demnach gibt es  $\#Q = n! / k_1! k_2! \dots k_\ell!$  Klassen (E237).

## Zweites Beispiel zur Klassengleichung

E308

**Beispiel:** Sei  $M$  eine Menge,  $X = M^2$  und  $\sigma : X \rightarrow X : (x, y) \mapsto (y, x)$ .



Dies definiert die grobe Zerlegung  $X = \text{fix}(\sigma) \sqcup \text{supp}(\sigma)$  und die feinere Bahnzerlegung  $Q = \{\{(x, y), (y, x)\} \mid (x, y) \in M^2\}$  bezüglich  $\sigma$ .

Es gilt  $\sigma \circ \sigma = \text{id}_X$ , daher hat jede Bahn die Länge entweder 1 oder 2:

$$\text{fix}(\sigma) = \bigsqcup Q_1 \quad \text{mit} \quad Q_1 = \{\{(x, x)\} \mid x \in M\},$$

$$\text{supp}(\sigma) = \bigsqcup Q_2 \quad \text{mit} \quad Q_2 = \{\{(x, y), (y, x)\} \mid x \neq y \text{ in } M\}.$$

Aus der Bahnengleichung folgt:

$$X = \text{fix}(\sigma) \sqcup \text{supp}(\sigma) \implies \#X = \#\text{fix}(\sigma) + 2 \cdot \#Q_2$$

**Satz E3D: Involutionen und Parität**

Wir nennen  $\sigma : X \rightarrow X$  eine **Involution auf  $X$** , wenn  $\sigma \circ \sigma = \text{id}_X$  gilt. Somit ist  $\sigma \in S_X$  eine Permutation, und jeder Zykel hat Länge 1 oder 2. Zum Beispiel ist  $\text{id}_X$  eine Involution, und jeder Punkt ist ein Fixpunkt.

Wir haben  $X = \text{fix}(\sigma) \sqcup \text{supp}(\sigma)$ . Ist  $X$  zudem endlich, so gilt

$$\#X = \# \text{fix}(\sigma) + 2t$$

und  $t \in \mathbb{N}$  ist die Anzahl der 2-Zykel. Demnach sind äquivalent:

- 1 Mindestens eine Involution  $\sigma : X \rightarrow X$  hat ungerade Fixpunktzahl.
- 2 Die Menge  $X$  hat ungerade Elementezahl, kurz  $\#X \in 2\mathbb{N} + 1$ .
- 3 Jede Involution  $\sigma : X \rightarrow X$  hat ungerade Fixpunktzahl.

**Beispiel:** Die Spiegelung  $\sigma : M^2 \rightarrow M^2 : (x, y) \mapsto (y, x)$  ist involutiv mit  $\text{fix}(\sigma) = \Delta_M = \{ (x, x) \mid x \in M \}$  und  $\text{supp}(\sigma) = \{ (x, y) \mid x \neq y \}$ . Also ist  $\#M^2$  ungerade genau dann, wenn  $\#M$  ungerade ist.

**Welche Zahlen sind Summe von zwei Quadraten?**

Erste experimentelle Daten:

$0 = 0^2 + 0^2$	$1 = 1^2 + 0^2$	$2 = 1^2 + 1^2$	$3 = \text{☹}$
$4 = 2^2 + 0^2$	$5 = 2^2 + 1^2$	$6 = \text{☹}$	$7 = \text{☹}$
$8 = 2^2 + 2^2$	$9 = 3^2 + 0^2$	$10 = 3^2 + 1^2$	$11 = \text{☹}$
$12 = \text{☹}$	$13 = 3^2 + 2^2$	$14 = \text{☹}$	$15 = \text{☹}$
$16 = 4^2 + 0^2$	$17 = 4^2 + 1^2$	$18 = 3^2 + 3^2$	$19 = \text{☹}$
$20 = 4^2 + 2^2$	$21 = \text{☹}$	$22 = \text{☹}$	$23 = \text{☹}$
$24 = \text{☹}$	$25 = 3^2 + 4^2$	$26 = 1^2 + 5^2$	$27 = \text{☹}$
$28 = \text{☹}$	$29 = 2^2 + 5^2$	$30 = \text{☹}$	$31 = \text{☹}$

**Übung:** Keine natürliche Zahl  $4k + 3$  ist Summe von zwei Quadraten. In  $\mathbb{Z}_4$  gilt  $\{ a^2 \mid a \in \mathbb{Z}_4 \} = \{0, 1\}$  und  $\{0, 1\} + \{0, 1\} = \{0, 1, 2\} \not\ni 3$ .

**Satz E3E: Fermats Zwei-Quadrate-Satz**

Jede Primzahl  $p$  der Form  $p = 4k + 1$  ist Summe von zwei Quadraten.

Dieser Abzähltrick ist sehr einfach, geradezu banal, doch wirkungsvoll! Abzählen ist gut, doppeltes Abzählen à la Klassengleichung ist besser.

Wir betrachten in Satz E3D nicht die genaue Elementezahl  $\#S$ , sondern nur die Parität:  $\#S$  ist entweder gerade oder ungerade. Aus der Bahngleichung  $\#X = \# \text{fix}(\sigma) + 2t$  mit  $t \in \mathbb{N}$  lesen wir die Implikationen „(1)  $\Rightarrow$  (2)  $\Rightarrow$  (3)“ ab. Für „(3)  $\Rightarrow$  (1)“ nutzen wir  $\sigma = \text{id}_X$ .

☺ Der Satz gilt genauso für jede Primzahl  $p \in \mathbb{N}_{\geq 2}$  und  $\sigma : X \rightarrow X$  mit  $\sigma^p = \text{id}_X$ . Jede Bahn hat dann entweder Länge 1 oder Länge  $p$ . Aus der Bahngleichung erhalten wir dann  $\#X = \# \text{fix}(\sigma) + pt$ . Ich diskutiere hier zunächst nur den einfachsten Fall  $p = 2$ .

**Ausblick:** Existenzsätze für Fixpunkte sind ein wichtiges Werkzeug der Mathematik. Hierzu ist Satz E3D eine erste schöne Illustration. In der Analysis lernen Sie Banachs Fixpunktsatz kennen und nutzen. Die Topologie erklärt Ihnen Brouwers Fixpunktsatz, die Algebraische Topologie noch allgemeiner den Lefschetzschen Fixpunktsatz; dieser hat eine frappierende Ähnlichkeit zum Involutionssatz E3D.

**Welche Zahlen sind Summe von zwei Quadraten?**

In dieser kleinen Tabelle springt sofort eine Beobachtung ins Auge: In der rechten Spalte treten, soweit wir sehen, keine Treffer auf. Wenn Sie möchten, können Sie dies nun allgemein beweisen. Hierzu betrachten Sie Quadrate in  $\mathbb{Z}_4$  ... Probieren Sie's!

Eine weitere Regelmäßigkeit dieser Tabelle ist etwas versteckt: In der zweiten Spalte treten augenscheinlich sehr viele Treffer auf. Nicht jede Zahl  $4k + 1$  ist Summe zweier Quadrate, doch viele sind's. Fermats berühmter Zwei-Quadrate-Satz besagt hierzu ganz allgemein: Jede Primzahl  $p$  der Form  $p = 4k + 1$  ist Summe von zwei Quadraten.

Kleine Beispiele probieren Sie leicht selbst oder mit einem Computer. Doch wie beweisen wir dies allgemein? Es gibt unendlich viele Fälle! Zu Fermats Zwei-Quadrate-Satz gibt es sehr viele schöne Beweise. Ich zeige Ihnen hier ein besonders kurzes und geniales Argument.

Ich verlange nicht, dass Sie sofort alle Details nachrechnen, vielmehr schlage ich vor, dass Sie zunächst die Beweisstruktur verstehen lernen... und ihre Eleganz bewundern!

Don Zagier: *A one-sentence proof that every prime  $p \equiv 1 \pmod{4}$  is a sum of two squares.* Amer. Math. Monthly 77 (1990), p. 144.

**A One-Sentence Proof That Every Prime  $p \equiv 1 \pmod{4}$  Is a Sum of Two Squares**

D. ZAGIER

Department of Mathematics, University of Maryland, College Park, MD 20742

The involution on the finite set  $S = \{(x, y, z) \in \mathbb{N}^3 : x^2 + 4yz = p\}$  defined by

$$\sigma : (x, y, z) \mapsto \begin{cases} (x + 2z, z, y - x - z) & \text{if } x < y - z \\ (2y - x, y, x - y + z) & \text{if } y - z < x < 2y \\ (x - 2y, x - y + z, y) & \text{if } x > 2y \end{cases}$$

$\text{fix}(\sigma) = \{(1, 1, (p-1)/4)\}$   $\tau :$

has exactly one fixed point, so  $|S|$  is odd and the involution defined by  $(x, y, z) \mapsto (x, z, y)$  also has a fixed point.  $\square \text{fix}(\tau) \ni (x, y, y) \Rightarrow p = x^2 + 4y^2 = x^2 + (2y)^2$

„The verifications of the implicitly made assertions... are immediate and have been left to the reader.“

**Aufgabe:** Zeigen Sie die hier implizit gemachten Behauptungen:

- (1) Die Menge  $S := \{(x, y, z) \in \mathbb{N}^3 \mid x^2 + 4yz = p\}$  ist endlich.
- (2) Die Menge  $S$  wird zerlegt gemäß  $S = S_1 \sqcup S_2 \sqcup S_3$  mit

$$S_1 = \{(x, y, z) \in S \mid x < y - z\}, \quad \sigma_1(x, y, z) = (x + 2z, z, y - x - z),$$

$$S_2 = \{(x, y, z) \in S \mid y - z < x < 2y\}, \quad \sigma_2(x, y, z) = (2y - x, y, x - y + z),$$

$$S_3 = \{(x, y, z) \in S \mid 2y < x\}, \quad \sigma_3(x, y, z) = (x - 2y, x - y + z, y).$$

- (3) Die hier angegebenen Formeln für  $\sigma_1, \sigma_2, \sigma_3 : \mathbb{Z}^3 \rightarrow \mathbb{Z}^3$  erfüllen  $\sigma_3 \circ \sigma_1 = \text{id}_{\mathbb{Z}^3}$  und  $\sigma_1 \circ \sigma_3 = \text{id}_{\mathbb{Z}^3}$  sowie  $\sigma_2 \circ \sigma_2 = \text{id}_{\mathbb{Z}^3}$ .
- (4) Es gilt  $\sigma_1(S_1) \subseteq S_3$  und  $\sigma_3(S_3) \subseteq S_1$  sowie  $\sigma_2(S_2) \subseteq S_2$ . Dies definiert die Involution  $\sigma : S \rightarrow S$  mit  $\sigma(u) = \sigma_i(u)$  für  $u \in S_i$ .
- (5) Es gilt  $\text{fix}(\sigma) = \{(1, 1, (p-1)/4)\}$ . Somit ist  $\#S$  ungerade.
- (6) Die Involution  $\tau : S \rightarrow S : (x, y, z) \mapsto (x, z, y)$  ist wohldefiniert.
- (7) Da  $\#S$  ungerade ist, ist auch  $\#\text{fix}(\tau)$  ungerade, also  $\text{fix}(\tau) \neq \emptyset$ .
- (8) Jeder Fixpunkt von  $\tau$  hat die Form  $(x, y, y)$  mit  $x^2 + (2y)^2 = p$ .

**Lösung:** (1) Aus  $(x, y, z) \in S$  folgt  $x, y, z \geq 1$ , da  $p$  prim ist. Daraus wiederum folgt  $x, y, z \in \{1, \dots, p\}$ , also grob  $\#S \leq p^3$ .

(2) Sei  $(x, y, z) \in S$ . Für  $x = 2y$  wäre  $p = 4y(y + z)$  nicht prim. Für  $x = y - z$  wäre  $p = y^2 + 2yz + z^2 = (y + z)^2$  ebenfalls nicht prim. Also gilt entweder  $x < y - z$  oder  $y - z < x < 2y$  oder  $2y < x$ .

(3,4) Definition einsetzen und sorgsam nachrechnen!

(5) Jeder Fixpunkt von  $\sigma$  liegt in  $S_2$ . Aus  $(x, y, z) = (2y - x, y, x - y + z)$  folgt  $x = y$ , also  $x(x + 4z) = p$  und somit  $x = y = 1$  und  $z = (p - 1)/4$ . Somit hat  $\sigma$  genau einen Fixpunkt:  $\text{fix}(\sigma) = \{(1, 1, (p - 1)/4)\}$ . Dank Bahnengleichung (Satz E3D) ist  $\#S$  ungerade.

(6) Aus  $(x, y, z) \in S$  folgt  $(x, z, y) \in S$ , also ist  $\tau$  wohldefiniert.

(7) Dies folgt erneut aus der Bahnengleichung (Satz E3D).

(8) Tatatata! Augen reiben und alles nochmal durchgehen... Die wunderschöne geometrische Interpretation dahinter erklären Ihnen Edmund Weitz, *Was ist Mathematik eigentlich?*, [youtu.be/u7XZDniQEj4](https://youtu.be/u7XZDniQEj4), Burkard Polster, *Fermats two square theorem*, [youtu.be/DjI1NICfj0k](https://youtu.be/DjI1NICfj0k).

Dieser Beweis-in-einem-Satz sagt uns nicht, wie man darauf kommt. Das ist die genial-kreative Leistung des Autors. Don Zagier schreibt:

This proof is a simplification of one due to Heath-Brown [1] (inspired, in turn, by a proof given by Liouville). The verifications of the implicitly made assertions—that  $S$  is finite and that the map is well-defined and involutory (i.e., equal to its own inverse) and has exactly one fixed point—are immediate and have been left to the reader. Only the last requires that  $p$  be a prime of the form  $4k + 1$ , the fixed point then being  $(1, 1, k)$ .

Note that the proof is not constructive: it does not give a method to actually find the representation of  $p$  as a sum of two squares. A similar phenomenon occurs with results in topology and analysis that are proved using fixed-point theorems. Indeed, the basic principle we used: “The cardinalities of a finite set and of its fixed-point set under any involution have the same parity,” is a combinatorial analogue and special case of the corresponding topological result: “The Euler characteristics of a topological space and of its fixed-point set under any continuous involution have the same parity.”

For a discussion of constructive proofs of the two-squares theorem, see the Editor’s Corner elsewhere in this issue.

REFERENCE

- 1. D. R. Heath-Brown, Fermat’s two-squares theorem, *Invariant* (1984) 3–5.

Wir nennen  $R_1 \subseteq X \times Y$  eine **Relation zwischen  $X$  und  $Y$** .

Wir nennen  $R_2 \subseteq X \times X$  eine **Relation auf der Menge  $X$** .

Sei  $X$  eine Menge und  $f : X \rightarrow Y$  eine Abbildung. Hierzu betrachten wir

$$(\sim) = R = R_f := \{ (x, y) \in X \times X \mid f(x) = f(y) \} \subseteq X \times X.$$

Infix-Notation  $x \sim y \Leftrightarrow f(x) = f(y)$ , gesprochen „ $x$  ist äquivalent zu  $y$ “.

Diese Relation erfreut sich folgender Eigenschaften für alle  $x, y, z \in X$ :

Reflexivität, **Refl**( $X, R$ ):  $\Delta_X \subseteq R, \quad x R x$

Symmetrie, **Sym**( $X, R$ ):  $R = R^T, \quad x R y \Rightarrow y R x$

Transitivität, **Tran**( $X, R$ ):  $R \bullet R \subseteq R, \quad x R y \wedge y R z \Rightarrow x R z$

Wir kehren nun die Sichtweise um und erheben dies zur Definition:

**Definition E3F: Äquivalenzrelation**

Eine Relation  $R \subseteq X \times X$  auf der Menge  $X$  heißt **Äquivalenzrelation**, wenn  $R$  reflexiv, symmetrisch und transitiv ist.

Die **Äquivalenzklasse** von  $x \in X$  bezüglich  $R$  ist die Menge

$$[x] = [x]_R := \{ y \in X \mid x R y \}.$$

Jede Äquivalenzklasse ist nicht-leer, denn  $x \in [x]_R$  dank Reflexivität.

Aus  $y \in [x]_R$  folgt  $[y]_R \subseteq [x]_R$  dank Transitivität, und dank Symmetrie  $[y]_R \supseteq [x]_R$ , insgesamt also  $[y]_R = [x]_R$ . Wir erhalten eine Zerlegung: **Je zwei Äquivalenzklassen sind entweder gleich oder disjunkt.**

Der **Quotient** von  $X$  bezüglich  $R$  ist die Menge aller Äquivalenzklassen:

$$X/R := \{ [x]_R \mid x \in X \}$$

Dies ist eine Zerlegung von  $X$ , also  $X/R \subseteq \mathfrak{P}(X)^*$  und  $X = \bigsqcup X/R$ . Jedes Element  $x \in X$  gehört zu genau einer Klasse  $c \in X/R$ .

Die zugehörige **Quotientenabbildung** oder **kanonische Surjektion** ist

$$q = q_R : X \twoheadrightarrow X/R : x \mapsto [x]_R.$$

Genau dann gilt  $q(x) = q(y)$ , wenn  $x R y$  gilt. Das bedeutet  $R_q = R$ .

**Proposition E3G: Zerlegungen entsprechen Äquivalenzrelationen.**

Jede Äquivalenzrelation  $R$  auf  $X$  definiert eine Zerlegung  $Q$  von  $X$ :

$$Q = Z(R) = X/R := \{ [x]_R \mid x \in X \}$$

Jede Zerlegung  $Q$  von  $X$  definiert eine Äquivalenzrelation  $R$  auf  $X$ :

$$R = A(Q) := \{ (x, y) \in X \times X \mid \exists C \in Q : x \in C \wedge y \in C \}$$

Dabei gilt  $A(Z(R)) = R$  und  $Z(A(Q)) = Q$ . Wir erhalten so die Bijektion

$$(A, Z) : \{ Q \subseteq \mathfrak{P}(X)^* \mid X = \bigsqcup Q \} \cong \{ R \subseteq X \times X \mid \Delta_X \subseteq R = R^T = R \bullet R \}$$

zwischen Zerlegungen von  $X$  und Äquivalenzrelationen auf  $X$ .

😊 Es ist hilfreich und bequem, beide Sichtweise nutzen zu können. Oft sind Äquivalenzrelationen bequemer, zum Beispiel in Satz E3H. Die Zerlegung  $Q$  nutzen wir zur Definition des Quotienten  $q : X \twoheadrightarrow Q$ .

Ist  $C \in X/R$  eine Äquivalenzklasse, so nennen wir jedes Element  $x \in C$  einen **Repräsentanten** der Klasse  $C$ . Die Wahl eines Repräsentanten ist im Allgemeinen vollkommen willkürlich, denn sie ist weder eindeutig noch irgendwie kanonisch, und im Allgemeinen auch nicht erforderlich:

😊 Die Quotientenkonstruktion wurde gerade dazu erschaffen, um uns von Repräsentanten zu befreien! Es lebe die Klasse!

Das klingt revolutionär, und die mathematische Abstraktion ist es auch: Statt mit Elementen  $x \in X$  arbeiten wir mit Äquivalenzklassen  $C \in X/R$ . Der Faktorisierungssatz E3J ist hierzu unser Universalwerkzeug.

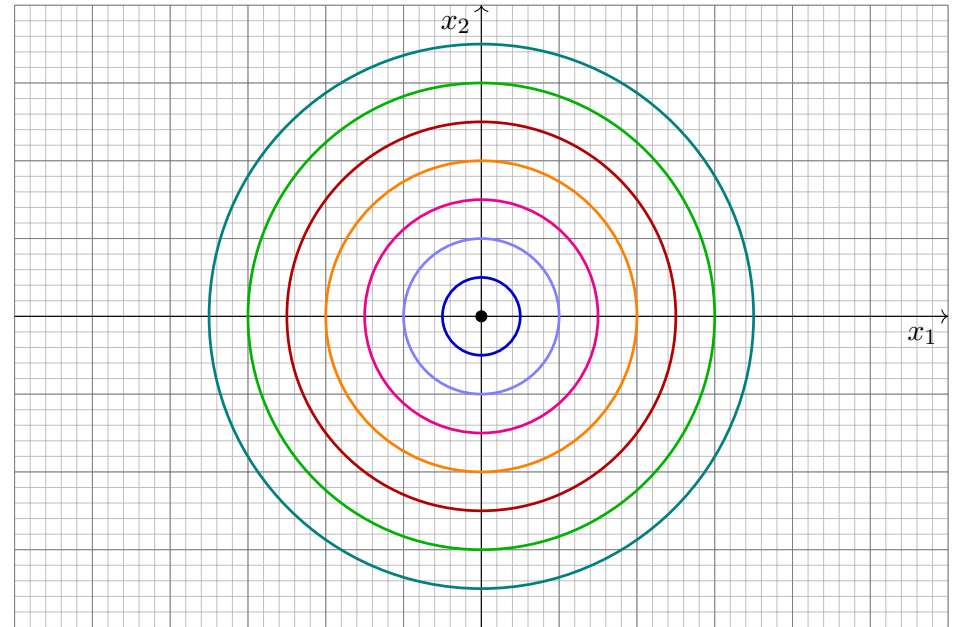
😊 Um diese Sichtweise zu betonen und didaktisch vorzubereiten, habe ich zunächst die Zerlegungen in den Vordergrund gestellt und möglichst ohne die Wahl von Repräsentanten gearbeitet.

**Beispiel:** Die grösste Äquivalenzrelation auf  $X$  ist  $G = X \times X$ . Sie ist reflexiv, symmetrisch, transitiv. (Größer als  $X \times X$  geht es nicht.) Für jedes Element  $a \in X$  gilt hier  $[a] = X$ , also  $X/G = \{ X \}$ . Die Quotientenabbildung  $q: X \rightarrow X/G: a \mapsto X$  ist konstant. Hier werden alle Elemente zu einer Klasse  $X$  zusammengefasst.

**Beispiel:** Die feinste Äquivalenzrelation ist  $F = \Delta_X = \{ (x, x) \mid x \in X \}$ : Sie ist reflexiv, symmetrisch, transitiv. (Kleiner als  $\Delta_X$  geht es nicht.) Für jedes Element  $a \in X$  gilt  $[a] = \{a\}$ , also  $X/F = \{ \{a\} \mid a \in X \}$ . Die Quotientenabbildung  $q: X \rightarrow X/F: a \mapsto \{a\}$  ist bijektiv. Hier werden keine Elemente zusammengefasst, jedes bleibt einzeln.

**Aufgabe:** Im  $\mathbb{R}^2$  betrachten wir  $|x| = \sqrt{x_1^2 + x_2^2}$  und  $u \sim v \Leftrightarrow |u| = |v|$ . Ist dies eine Äquivalenzrelation? Was sind hier die Äquivalenzklassen?

**Lösung:** (1) Ja, diese Relation  $\sim$  ist reflexiv, symmetrisch, transitiv:  
 $|u| = |u|$ ,  $|u| = |v| \Rightarrow |v| = |u|$ ,  $|u| = |v| \wedge |v| = |w| \Rightarrow |u| = |w|$ .  
 (2) Äq'klassen sind Kreislinien  $S_r = \{ (x_1, x_2) \in \mathbb{R}^2 \mid x_1^2 + x_2^2 = r^2 \}$ .



**Satz E3H:** die erzeugte Äquivalenzrelation

Jede Relation  $P \subseteq X \times X$  erzeugt eine Äquivalenzrelation  $T \subseteq X \times X$ :

$$\begin{aligned}
 P &\mapsto R := P \cup \Delta_X \\
 &\mapsto S := R \cup R^T = P \cup \Delta_X \cup P^T \\
 &\mapsto T := \bigcup_{n \in \mathbb{N}} S^{\bullet n} = \Delta_X \cup S \cup (S \bullet S) \cup (S \bullet S \bullet S) \cup \dots
 \end{aligned}$$

Damit ist  $T$  die kleinste Äquivalenzrelation auf  $X$ , die  $P$  enthält. Wir nennen  $T$  die von  $P$  auf  $X$  **erzeugte Äquivalenzrelation**.

**Aufgabe:** Auf  $X = \mathbb{R}$  definieren wir  $P$  durch  $a P b \Leftrightarrow b - a = 1$ . Ist  $P$  reflexiv? symmetrisch? transitiv? Bestimmen Sie  $R, S, T$ .

**Lösung:**  $P$  ist weder reflexiv noch symmetrisch noch transitiv. Wir finden  $a R b \Leftrightarrow b - a \in \{0, 1\}$ : Diese Relation ist reflexiv. Wir finden  $a S b \Leftrightarrow b - a \in \{0, \pm 1\}$ : reflexiv und symmetrisch. Wir finden  $a T b \Leftrightarrow b - a \in \mathbb{Z}$ : reflexiv, symmetrisch und transitiv.

Im ersten Schritt  $P \mapsto R = P \cup \Delta_X$  machen wir  $R$  reflexiv, im zweiten  $R \mapsto S = R \cup R^T$  bilden wir die reflexiv-symmetrische Hülle  $S$  zu  $P$ , im dritten  $S \mapsto T = \bigcup_{n \in \mathbb{N}} S^{\bullet n}$  bilden wir die transitive Hülle  $T$  von  $S$ .

😊 Ebenso genügt  $S = P \cup P^T$  und  $T = \bigcup_{n \in \mathbb{N}} S^{\bullet n}$ , denn  $S^{\bullet 0} = \text{id}_X$ .

**Übung:** (1) Zeigen Sie, dass  $T$  eine Äquivalenzrelation auf  $X$  ist. (2) Zudem ist  $T$  die kleinste Äquivalenzrelation, die  $P$  enthält.

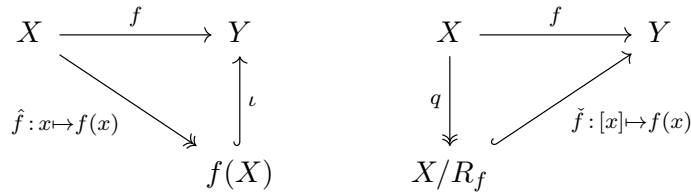
**Lösung:** (1) Die Relation  $S$  ist reflexiv und symmetrisch, also auch  $T$ . Zudem ist  $T$  sogar transitiv: Wenn wir in endlich vielen  $S$ -Schritten von  $x$  nach  $y$  gelangen und von  $y$  nach  $z$ , dann auch von  $x$  nach  $z$ .

(2) Wir betrachten die Menge aller Äq'relationen auf  $X$ , die  $P$  enthalten:

$$\mathcal{A} = \{ V \subseteq X \times X \mid V \text{ ist Äq'relation mit } V \supseteq P \}$$

Die größte solche Äq'relationen ist  $X \times X \in \mathcal{A}$ , die kleinste ist  $T$ : Dank (1) gilt  $T \in \mathcal{A}$ . Für  $V \in \mathcal{A}$  gilt  $P \subseteq V$ , also  $S \subseteq V$  und  $T \subseteq V$ .

😊 Somit erhalten wir die alternative Konstruktion  $T = \bigcap \mathcal{A}$ .



Gegeben sei  $f : X \rightarrow Y$ , im Allgemeinen weder injektiv noch surjektiv.

**Surjektiv machen:** Wir gehen von  $f : X \rightarrow Y$  zu  $\hat{f} : X \twoheadrightarrow f(X)$  über. Wir erhalten die Faktorisierung  $f = \iota \circ \hat{f}$  in Surjektion und Inklusion.

**Injektiv machen:** Die Abbildung  $f$  definiert ihre Äquivalenzrelation

$$R_f := \{ (x, x') \in X \times X \mid f(x) = f(x') \}.$$

Die Abbildung  $\check{f} : X/R_f \rightarrow Y : [x] \mapsto f(x)$  ist wohldefiniert und injektiv. Wir erhalten die Faktorisierung  $f = \check{f} \circ q$  in Quotient und Injektion.

Hierbei ist  $\hat{f}$  surjektiv, und zudem injektiv gdw  $f$  injektiv ist. Ebenso ist  $\check{f}$  injektiv, und zudem surjektiv gdw  $f$  surjektiv ist.

Die Konstruktion von  $\hat{f} : X \twoheadrightarrow f(X)$  entsteht aus  $f$  durch Einschränkung der Zielmenge  $Y$  auf das Bild  $f(X)$ , siehe D306.

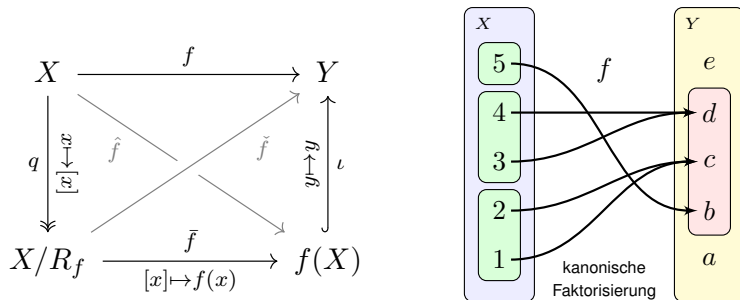
Dual hierzu: Die Konstruktion von  $\check{f}$  nutzt den Quotienten  $X/R_f$ .

(1) Wohldefiniertheit: Aus  $[x] = [x']$  folgt  $f(x) = f(x')$ .

Das ist ein einfacher Spezialfall des Faktorisierungssatzes E3J.

(2) Injektivität: Gleichheit  $\check{f}(c) = \check{f}(c')$  bedeutet: Für Repräsentanten  $x \in c$  und  $x' \in c'$  gilt  $f(x) = f(x')$ , daraus folgt  $(x, x') \in R_f$  also  $c = c'$ .

Der folgende Satz leistet beides zugleich: injektiv und surjektiv machen! Dies nennt man die kanonische Faktorisierung.



**Satz E3I: die kanonische Faktorisierung**

Jede Abbildung  $f : X \rightarrow Y$  faktorisiert gemäß  $f = \iota \circ \bar{f} \circ q$  in

- 1 die Quotientenabbildung  $q : X \twoheadrightarrow X/R_f : x \mapsto [x]$ ,
- 2 die Bijektion  $\bar{f} : X/R_f \xrightarrow{\sim} f(X) : [x] \mapsto f(x)$ ,
- 3 die Inklusion  $\iota : f(X) \hookrightarrow Y : y \mapsto y$ .

Im Beispiel oben gilt  $X/R_f = \{\{1, 2\}, \{3, 4\}, \{5\}\}$  und  $f(X) = \{b, c, d\}$  sowie  $\bar{f} : X/R_f \rightarrow f(X) : \{1, 2\} \mapsto c, \{3, 4\} \mapsto d, \{5\} \mapsto b$ .

😊 So können wir jede beliebige Abbildung  $f : X \rightarrow Y$  kanonisch zerlegen in die drei einfacheren Abbildungen  $q, \bar{f}, \iota$ . Diese heißen daher **kanonische Surjektion / Bijektion / Injektion**.

**Beweis:** Die Abbildungen  $q$  und  $\bar{f}$  und  $\iota$  sind wohldefiniert.

Für Quotient  $q$  und Inklusion  $\iota$  ist dies klar nach Konstruktion.

Für  $\bar{f}$  folgt dies aus dem Faktorisierungssatz E3J oder hier direkt:

(0) Wohldefiniertheit: Aus  $[x] = [x']$  folgt  $f(x) = f(x')$ .

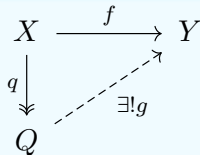
(1) Injektivität: Gleichheit  $\bar{f}(c) = \bar{f}(c')$  bedeutet: Für Repräsentanten  $x \in c$  und  $x' \in c'$  gilt  $f(x) = f(x')$ , daraus folgt  $(x, x') \in R_f$  also  $c = c'$ .

(2) Surjektivität: Zu jedem Bildelement  $y \in f(X)$  existiert mindestens ein Urbild  $x \in X$  mit  $f(x) = y$ . Somit gilt auch  $\bar{f}([x]) = y$ . ◻

😊 Diese Zerlegung haben wir in Satz E2L erfolgreich genutzt, um Injektionen und Surjektionen zu zählen. Sie ist auch sonst oft nützlich und allgemein ein gutes Organisationsprinzip. Sie sehen im Verlauf Ihres Studiums immer wieder Anwendungen dieser Faktorisierung.

**Satz E3J: eindeutige Faktorisierung über eine Surjektion**

Sei  $q: X \twoheadrightarrow Q$  eine Surjektion, etwa ein Quotient.  
Gegeben sei eine beliebige Abbildung  $f: X \rightarrow Y$ .



Zu  $(f, q)$  suchen wir eine **Faktorisierung**  $g: Q \rightarrow Y$  mit  $f = g \circ q$ , also  $f(x) = g(q(x))$  für alle  $x \in X$ .

**Eindeutigkeit:** Je zwei Faktorisierungen  $g, g': Q \rightarrow Y$  sind gleich.  
Zu jedem Element  $\bar{x} \in Q$  existiert ein Urbild  $x \in X$  mit  $q(x) = \bar{x}$ :

$$g(\bar{x}) = g(q(x)) = (g \circ q)(x) = (g' \circ q)(x) = g'(q(x)) = g'(\bar{x})$$

**Existenz:** Genau dann existiert  $g: Q \rightarrow Y$  mit  $f = g \circ q$ , wenn  $R_q \subseteq R_f$ :

Kompatibilität:  $\forall x, x' \in X : q(x) = q(x') \Rightarrow f(x) = f(x')$

In diesem Falle konstruieren wir  $g$  wie folgt: Zu jedem  $\bar{x} \in Q$  wählen wir willkürlich ein Urbild  $x \in X$  mit  $q(x) = \bar{x}$  und setzen  $g(\bar{x}) := f(x)$ .

$$g = f \circ q^{-1} = (Q, G, Y), \quad G = \{ (\bar{x}, y) \mid \exists x \in X : q(x) = \bar{x} \wedge f(x) = y \}$$

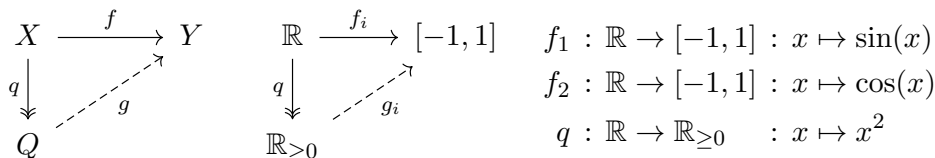
Im Falle  $f = g \circ q$  sagen wir  $f$  **faktoriert über  $q$  zu  $g$**  oder auch  $f: X \rightarrow Y$  **induziert  $g: Q \rightarrow Y$  über  $q: X \twoheadrightarrow Q$** . Die Relation  $g = f \circ q^{-1}$  ist linkstotal, da  $q$  surjektiv ist, und rechtseindeutig, da  $f$  kompatibel ist.

Die Bildmenge  $f(X) = g(Q)$  in  $Y$  bleibt dabei unverändert.  
Genau dann ist  $g$  injektiv, wenn  $R_q = R_f$  gilt.

**Beispiel:** Speziell sei  $q: X \rightarrow X/R$  ein Quotient. Genau dann faktoriert  $f: X \rightarrow Y$  über  $q$  zu  $g: X/R \rightarrow Y$ , wenn  $R \subseteq R_f$  gilt. In diesem Fall ist  $g$  eindeutig und wohldefiniert durch  $g([x]_R) = f(x)$ .

☺ Der Faktorisierungssatz ist das Universalwerkzeug, um Abbildungen  $g: Q \rightarrow Y$  auf der Quotientenmenge  $Q$  zu konstruieren: Nahezu jede Konstruktion verläuft genau so! Wie sollte es auch anders gehen?

Auf die Elemente der Quotientenmenge  $Q = X/R$ , also die Äq'-klassen  $C = q(x)$ , haben wir meist keinen direkten Zugriff, sondern nur über Repräsentanten  $x \in C$ . Wir definieren daher  $g: Q \rightarrow Y$  mit Hilfe von Repräsentanten. Hier sagt uns Satz E3J genau, was zu tun ist.



**Aufgabe:** Finden Sie alle Faktorisierungen  $g_1, g_2: \mathbb{R}_{\geq 0} \rightarrow [-1, 1]$

- mit  $f_1 = g_1 \circ q$ , also  $\sin(x) = g_1(x^2)$  für alle  $x \in \mathbb{R}$ ;
- mit  $f_2 = g_2 \circ q$ , also  $\cos(x) = g_2(x^2)$  für alle  $x \in \mathbb{R}$ .

**Lösung:** Wir wenden den Faktorisierungssatz E3J an:

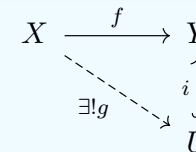
- Es gibt keine Faktorisierung  $g_1$ , denn  $f_1$  ist nicht kompatibel mit  $q$ . Zum Beispiel gilt  $q(-1) = q(+1)$ , aber  $\sin(-1) \neq \sin(+1)$ .
- Es gibt genau eine Faktorisierung  $g_2$ , denn  $f_2$  ist kompatibel mit  $q$ . Explizit gilt  $g_2(y) = \cos(\sqrt{y})$ . Die Analysis zeigt Ihnen noch mehr:

$$\cos(x) = \sum_{k=0}^{\infty} (-1)^k \frac{x^{2k}}{(2k)!} \implies g_2(y) = \sum_{k=0}^{\infty} (-1)^k \frac{y^k}{(2k)!}$$

Dual zur Faktorisierung über eine Surjektion wie in Satz E3J können wir über eine Injektion faktorisieren. Das ist wesentlich einfacher:

**Satz E3K: eindeutige Faktorisierung über eine Injektion**

Sei  $i: U \hookrightarrow Y$  eine Injektion, etwa eine Inklusion.  
Gegeben sei eine beliebige Abbildung  $f: X \rightarrow Y$ .



Zu  $(f, i)$  suchen wir eine **Faktorisierung**  $g: X \rightarrow U$  mit  $f = i \circ g$ , also  $f(x) = i(g(x))$  für alle  $x \in X$ .

**Eindeutigkeit:** Je zwei Faktorisierungen  $g, g': X \rightarrow U$  sind gleich. Aus  $f(x) = i(g(x)) = i(g'(x))$  folgt  $g(x) = g'(x)$  dank Injektivität von  $i$ .

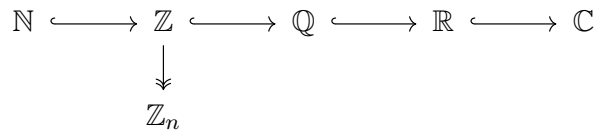
**Existenz:** Genau dann existiert  $g: X \rightarrow U$  mit  $f = i \circ g$ , wenn  $f(X) \subseteq i(U)$  gilt. In diesem Falle setzen wir  $g(x) = i^{-1}(f(x))$ , also:

$$g = i^{-1} \circ f = (X, G, U), \quad G = \{ (x, u) \mid f(x) = i(u) \}$$

**Wichtiger Spezialfall:** Ist  $\iota: U \subseteq Y$  eine Inklusion und  $f(X) \subseteq U$ , so ist  $g = f|_X^U$  die Einschränkung von  $f$  auf die Zielmenge  $U$ , siehe D306.



Auf Grundlage der Mengenlehre bauen wir das Zahlensystem auf:



Die **natürlichen Zahlen**  $(\mathbb{N}, +, 0, \cdot, 1)$  sind ein kommutativer Halbring; dabei erfüllt  $(\mathbb{N}, 0, s)$  mit  $s: n \mapsto n + 1$  die Dedekind–Peano–Axiome.

Die **ganzen Zahlen**  $(\mathbb{Z}, +, 0, \cdot, 1)$  sind ein kommutativer Ring mit  $\mathbb{N} \subset \mathbb{Z}$  als Teilhalbring und  $\mathbb{Z} = \{z = a - b \mid a, b \in \mathbb{N}\}$ .

Die **rationalen Zahlen**  $(\mathbb{Q}, +, 0, \cdot, 1)$  sind ein Körper mit  $\mathbb{Z} \subset \mathbb{Q}$  als Teilring und  $\mathbb{Q} = \{q = z/n \mid z, n \in \mathbb{Z}, n \neq 0\}$ .

Die **reellen Zahlen**  $(\mathbb{R}, +, 0, \cdot, 1)$  sind ein Körper mit  $\mathbb{Q} \subset \mathbb{R}$  und vollständig geordnet durch  $x \leq y \Leftrightarrow \exists a \in \mathbb{R}: x + a^2 = y$ .

Die **komplexen Zahlen**  $(\mathbb{C}, +, 0, \cdot, 1)$  sind ein Körper mit  $\mathbb{R} \subset \mathbb{C}$  dabei gilt  $\mathbb{C} = \mathbb{R}[i] = \{z = x + iy \mid x, y \in \mathbb{R}\}$  mit  $i^2 = -1$ .

Jede dieser Erweiterungen  $\mathbb{N} \hookrightarrow \mathbb{Z}$  und  $\mathbb{Z} \hookrightarrow \mathbb{Q}$  sowie  $\mathbb{Q} \hookrightarrow \mathbb{R}$  erschafft einen neuen Zahlbereich durch eine geeignete Quotientenkonstruktion! Das ist weit raffinierter als man auf den ersten Blick erwarten würde. Wenn später einmal Zeit dazu ist, will ich dies gerne für Sie ausarbeiten; im Folgenden führe ich nur den Übergang von  $\mathbb{Z}$  zu  $\mathbb{Q}$  beispielhaft aus.

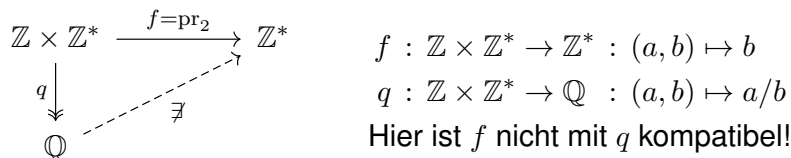
Die Erweiterung  $\mathbb{R} \hookrightarrow \mathbb{C}$  ist im Vergleich dazu sehr viel einfacher: Hier genügen Paare  $\mathbb{C} = \mathbb{R}^2$ , denn jede komplexe Zahl  $z \in \mathbb{C}$  schreibt sich *eindeutig* als  $z = x + yi$ . Auf diesen Paaren  $(x, y)$  reeller Zahlen definieren wir *unmittelbar* die Addition  $(x, y) + (u, v) := (x + u, y + v)$  und die Multiplikation  $(x, y) \cdot (u, v) := (xu - yv, xv + yu)$ , ganz direkt.

Psychologisch wird Ihnen die Schwierigkeit umgekehrt erscheinen, da sie sich an die schwierigeren Konstruktionen  $\mathbb{N} \hookrightarrow \mathbb{Z} \hookrightarrow \mathbb{Q} \hookrightarrow \mathbb{R}$  bereits lange gewöhnt haben, aber die leichtere Konstruktion  $\mathbb{R} \hookrightarrow \mathbb{C}$  für Sie noch ganz neu ist. Die mathematische Schwierigkeit jedoch, der Konstruktionsaufwand, ist im letzten Schritt am geringsten.

**Aufgabe:** Gegeben seien ganze Zahlen  $a \in \mathbb{Z}$  und  $b \in \mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$ . Was ist der Nenner des Bruchs  $c = a/b$  in  $\mathbb{Q}$ ? Speziell für  $c = 4/6$ ? Ist die Antwort wohldefiniert? Wo genau liegt das Problem?

**Lösung:** Naive Antwort: „Der Nenner von  $c = a/b$  ist die Zahl  $b$ .“ Der Nenner von  $c = 4/6$  wäre demnach die ganze Zahl 6. Ebenso gilt  $c = 6/9$ , der Nenner von  $c$  wäre also 9. Es gilt aber  $6 \neq 9$ . Die Antwort ist nicht wohldefiniert!

⚠ Der Versuch  $N: \mathbb{Q} \rightarrow \mathbb{Z}: a/b \mapsto b$  scheitert. Dies ist keine Funktion! Der Faktorisierungssatz E3J benennt genau das Problem:



😊 Jeder Bruch  $c = a/b \in \mathbb{Q}$  erlaubt eine Darstellung  $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$  als ein Paar (Zähler, Nenner). 😞 Diese Darstellung ist nicht eindeutig!

Niemand kann sagen, was „der“ Zähler und „der“ Nenner eines Bruchs sind: Diese Begriffe sind nicht wohldefiniert, wie wir gesehen haben. Wer es dennoch versucht, verwickelt sich in Widersprüche.

Wir können (mehr oder minder willkürliche) Wahlen treffen. Zum Beispiel könnten Sie hier vorschlagen, zu jedem Bruch  $c \in \mathbb{Q}$  seine vollständig gekürzte Darstellung  $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$  zu betrachten, also  $\text{ggT}(a, b) = 1$  und  $b > 0$ . Dieser Repräsentant ist tatsächlich eindeutig. Wir könnten damit Zähler und Nenner von  $c$  definieren durch  $Z(c) = a$  und  $N(c) = b$ . Im Beispiel wäre dann  $Z(4/6) = Z(6/9) = 2$  und  $N(4/6) = N(6/9) = 3$ .

Auch diese gutgemeinte Antwort ist leider nur eine scheinbare Lösung. Versuchen Sie beispielsweise  $1/2$  und  $1/3$  zu addieren; dazu möchten Sie zuerst die beiden Brüche „auf einen gemeinsamen Nenner bringen.“ Sie merken sofort, auch diese Sprechweise gerät hier schnell in Not. Es ist zwar möglich, aber wir müssten uns extrem verrenken.

😊 Diese Problematik erlaubt nur eine einzige vernünftige Lösung: Brüche sind Äquivalenzklassen!

Wir wollen den Ring  $(\mathbb{Z}, +, \cdot)$  in einen Körper  $(\mathbb{Q}, +, \cdot)$  einbetten.  
Idee: Wir rechnen mit Brüchen „ $a/b$ “. Das sind Äquivalenzklassen!

$$2/3 = 4/6 = 6/9 = 8/12 = \dots \quad \text{allgemein: } a/b = c/d \Leftrightarrow ad = cb$$

Brüche stellen wir dar durch Paare (Zähler, Nenner) bis auf Äquivalenz:

$$P = \mathbb{Z} \times \mathbb{Z}^* \quad \text{mit} \quad (a, b) \sim (c, d) \Leftrightarrow ad = cb.$$

**Aufgabe:** Ist diese Relation  $\sim$  eine Äquivalenzrelation?

**Lösung:** Reflexiv: Es gilt  $(a, b) \sim (a, b)$ , denn  $ab = ab$ .

Symmetrisch:  $(a, b) \sim (c, d) \Leftrightarrow ad = cb \Leftrightarrow cb = ad \Leftrightarrow (c, d) \sim (a, b)$ .

Transitiv: Aus  $(a, b) \sim (c, d)$  und  $(c, d) \sim (e, f)$  folgt  $ad = cb$  und  $cf = ed$ , also  $adf = cbf = cfb = edb$ . Den Faktor  $d \in \mathbb{Z}^*$  können wir kürzen!

Daraus folgt  $af = eb$ , also  $(a, b) \sim (e, f)$ .

Wir definieren so die Quotientenmenge  $Q := P/\sim$  und die zugehörige Quotientenabbildung  $q: P \twoheadrightarrow Q: (a, b) \mapsto [a, b]$ , suggestiv  $a/b := [a, b]$ .

Brüche  $a/b := [a, b]$  sind Äquivalenzklassen!

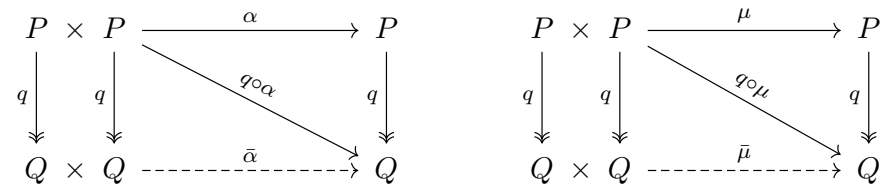
$$Q := P/\sim \quad \text{mit} \quad P = \mathbb{Z} \times \mathbb{Z}^* \quad \text{und} \quad (a, b) \sim (c, d) \Leftrightarrow ad = cb$$

Addition und Multiplikation definieren wir zunächst für Paare:

$$+ = \alpha : P \times P \rightarrow P : ((a, b), (c, d)) \mapsto (ad + cb, bd)$$

$$\cdot = \mu : P \times P \rightarrow P : ((a, b), (c, d)) \mapsto (ac, bd)$$

Sind diese Verknüpfungen kompatibel mit der Quotientenabbildung  $q$ ?



Für die Verknüpfungen  $\bar{\alpha}$  und  $\bar{\mu}$  wählen wir willkürlich Repräsentanten und verknüpfen diese in  $P$ . Ist das Ergebnis in  $Q$  wohldefiniert?

**Beispiel:** Führen willkürliche Wahlen zu verschiedenen Ergebnissen?

$$\frac{2}{3} + \frac{7}{8} = \frac{2 \cdot 8 + 7 \cdot 3}{3 \cdot 8} = \frac{37}{24}$$

$$\frac{4}{6} + \frac{-7}{-8} = \frac{4 \cdot (-8) + (-7) \cdot 6}{6 \cdot (-8)} = \frac{-74}{-48}$$

Gegeben seien jeweils äquivalente Darstellungen  $(a, b) \sim (a', b')$  und  $(c, d) \sim (c', d')$ , das heißt  $ab' = a'b$  und  $cd' = c'd$ . Wir müssen zeigen:

$$(a, b) + (c, d) = (ad + cb, bd) \quad \sim \quad (a', b') + (c', d') = (a'd' + c'b', b'd')$$

$$(a, b) \cdot (c, d) = (ac, bd) \quad \sim \quad (a', b') \cdot (c', d') = (a'c', b'd')$$

Alle Definitionen liegen explizit vor. Prüfen wir es nach!

$$(ad + cb)(b'd') = adb'd' + cbb'd' = a'bdd' + c'dbb' = (a'd' + c'b')(bd)$$

$$acb'd' = a'c'bd$$

😊 Nun genügt geduldiges Nachrechnen der Körperaxiome für  $(\mathbb{Q}, +, \cdot)$ . Der folgende Satz fasst diese Konstruktion allgemein zusammen.

**Satz E3L:** Einbettung eines Integritätsrings in seinen Bruchkörper

Sei  $(R, +, 0, \cdot, 1)$  ein Integritätsring, etwa die ganzen Zahlen  $\mathbb{Z}$  oder ein Polynomring  $K[X]$  über einem Körper  $K$ . Dann können wir  $R$  einbetten in einen Körper  $(Q, +, 0, \cdot, 1)$ , sodass  $Q = \{ a/b \mid (a, b) \in R \times R^* \}$  gilt.

**Konstruktion:** Wir nutzen Paare (Zähler, Nenner) bis auf Äquivalenz:

$$Q := P/\sim \quad \text{mit} \quad P = R \times R^* \quad \text{und} \quad (a, b) \sim (c, d) \Leftrightarrow ad = cb$$

Dies ist eine Äquivalenzrelation, transitiv dank Kürzungsregel in  $R$ .

Sei  $q: P \twoheadrightarrow Q: (a, b) \mapsto [a, b]$  die zugehörige Quotientenabbildung.

Wir haben die Einbettung  $R \hookrightarrow Q: a \mapsto [a, 1]$  und schreiben kurz  $R \subseteq Q$ .

Addition und Multiplikation definieren wir zunächst für Paare:

$$+ : P \times P \rightarrow P : ((a, b), (c, d)) \mapsto (ad + cb, bd)$$

$$\cdot : P \times P \rightarrow P : ((a, b), (c, d)) \mapsto (ac, bd)$$

Diese Verknüpfungen sind kompatibel mit der Quotientenabbildung

$q: P \twoheadrightarrow Q$ , daher definieren sie eine Addition und Multiplikation auf  $Q$ .

Damit ist  $(Q, +, 0, \cdot, 1)$  ein Körper und  $Q = \{ a/b \mid (a, b) \in R \times R^* \}$ .

Sei  $n \in \mathbb{Z}$  eine ganze Zahl. Wir betrachten die Menge aller Vielfachen:

$$H = n\mathbb{Z} := \{ nk \mid k \in \mathbb{Z} \}$$

Diese erfreut sich folgender Eigenschaften:

- 1 Es gilt  $0 \in H$ ,  
denn  $0 = n \cdot 0$ .
- 2 Aus  $a \in H$  folgt  $-a \in H$ ,  
denn aus  $a = nk$  folgt  $-a = n \cdot (-k)$ .
- 3 Aus  $a, b \in H$  folgt  $a + b \in H$ ,  
denn aus  $a = nk$  und  $b = n\ell$  folgt  $a + b = n(k + \ell)$ .

😊 Zusammenfassend sagen wir hierzu:  $(\mathbb{Z}, +, 0, -)$  ist eine kommutative Gruppe, und hierin ist  $H \subseteq \mathbb{Z}$  eine Untergruppe.

Für die Multiplikation halten wir etwas allgemeiner fest:

Aus  $a \in H$  folgt  $ua \in H$  für alle  $u \in \mathbb{Z}$ , denn  $u(nk) = n(uk)$ .

Auf der Menge  $\mathbb{Z}$  definieren wir die Relation „ $a$  kongruent  $b$  modulo  $n$ “:

$$a \equiv b \Leftrightarrow a \equiv_n b \quad :\Leftrightarrow \quad a - b \in n\mathbb{Z}$$

Dies ist eine Äquivalenzrelation:

- 1 Reflexivität: Es gilt  $a \equiv a$ , denn  $a - a = 0 \in H$ .
- 2 Symmetrie:  $a \equiv b$  bedeutet  $a - b \in H$ , also  $b - a \in H$ , somit  $b \equiv a$ .
- 3 Transitivität:  $a \equiv b$  und  $b \equiv c$  bedeuten  $a - b \in H$  und  $b - c \in H$ , daraus folgt  $H \ni (a - b) + (b - c) = a - c$ , somit  $a \equiv c$ .

😊 Die drei definierenden Eigenschaften der Untergruppe  $H \subseteq \mathbb{Z}$  übersetzen sich direkt in Reflexivität, Symmetrie und Transitivität.

**Bemerkung:** Wir nutzen den Rest  $p: \mathbb{Z} \rightarrow \mathbb{Z}_n: a \mapsto a \bmod n$ .

Damit ist die Bedingung  $a - b \in n\mathbb{Z}$  äquivalent zu  $p(a) = p(b)$ .

Auch daraus folgt sofort Reflexivität, Symmetrie und Transitivität.

Zu jeder ganzen Zahl  $a \in \mathbb{Z}$  haben wir die zugehörige Äquivalenzklasse:

$$[a] = a + n\mathbb{Z} := \{ a + nk \mid k \in \mathbb{Z} \}$$

Alle Äquivalenzklassen fassen wir zur Quotientenmenge zusammen:

$$\mathbb{Z}/n = \mathbb{Z}/n\mathbb{Z} := \{ [a] = a + n\mathbb{Z} \mid a \in \mathbb{Z} \}$$

Die zugehörige Quotientenabbildung ist demnach:

$$q: \mathbb{Z} \twoheadrightarrow \mathbb{Z}/n\mathbb{Z} : a \mapsto [a] = a + n\mathbb{Z}$$

**Beispiel:** Für  $n = 0$  erhalten wir  $\mathbb{Z}/0\mathbb{Z} = \{ \{a\} \mid a \in \mathbb{Z} \}$ .

Die Quotientenabbildung  $q: \mathbb{Z} \rightarrow \mathbb{Z}/0\mathbb{Z}: a \mapsto \{a\}$  ist bijektiv.

Hier gibt es nur ein Repräsentantensystem, nämlich die Menge  $\mathbb{Z}$ .

**Beispiel:** Für  $n = 1$  erhalten wir  $\mathbb{Z}/1\mathbb{Z} = \{ \mathbb{Z} \}$ .

Die Quotientenabbildung  $q: \mathbb{Z} \rightarrow \mathbb{Z}/1\mathbb{Z}: a \mapsto \mathbb{Z}$  ist konstant.

Für jedes Element  $a \in \mathbb{Z}$  ist somit  $\{a\}$  ein Repräsentantensystem.

Diese beiden Extremfälle kommen also natürlich vor, siehe E321.

**Beispiel:** Für  $n = 2$  haben wir genau zwei Äquivalenzklassen:

$$\begin{aligned} \mathbb{Z}/2\mathbb{Z} &= \{ 0 + 2\mathbb{Z} = \{ \dots, -4, -2, 0, 2, 4, 6, \dots \}, \\ &\quad 1 + 2\mathbb{Z} = \{ \dots, -3, -1, 1, 3, 5, 7, \dots \} \} \end{aligned}$$

Mögliche Repräsentantensysteme sind  $\{0, 1\}$  oder  $\{8, -5\} \dots$

**Beispiel:** Für  $n = 3$  haben wir genau drei Äquivalenzklassen:

$$\begin{aligned} \mathbb{Z}/3\mathbb{Z} &= \{ 0 + 3\mathbb{Z} = \{ \dots, -6, -3, 0, 3, 6, 9, \dots \}, \\ &\quad 1 + 3\mathbb{Z} = \{ \dots, -5, -2, 1, 4, 7, 10, \dots \}, \\ &\quad 2 + 3\mathbb{Z} = \{ \dots, -4, -1, 2, 5, 8, 11, \dots \} \} \end{aligned}$$

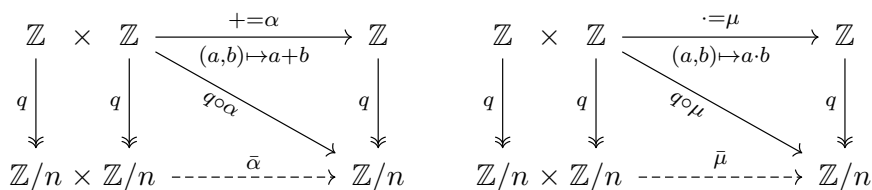
Mögliche Repräsentantensysteme sind  $\{0, 1, 2\}$  oder  $\{-1, 0, 1\} \dots$

**Beispiel:** Für jede ganze Zahl  $n \in \mathbb{Z}_{\geq 1}$  erhalten wir die Zerlegung

$$\mathbb{Z} = \bigsqcup \mathbb{Z}/n\mathbb{Z} = (n\mathbb{Z}) \sqcup (1 + n\mathbb{Z}) \sqcup \dots \sqcup (n - 1 + n\mathbb{Z}).$$

Das kanonische Repräsentantensystem ist  $\mathbb{Z}_n = \{0, 1, \dots, n - 1\}$ .

**Übung:** Sind Addition und Multiplikation in  $\mathbb{Z}$  kompatibel mit  $q$ ?



Für die Verknüpfungen  $\bar{\alpha}$  und  $\bar{\mu}$  wählen wir willkürlich Repräsentanten und verknüpfen diese in  $\mathbb{Z}$ . Ist das Ergebnis in  $\mathbb{Z}/n$  wohldefiniert?

Erst mit dieser Garantie erhalten wir auf  $\mathbb{Z}/n$  die Verknüpfungen

$$+ : \mathbb{Z}/n \times \mathbb{Z}/n \rightarrow \mathbb{Z}/n : [a] + [b] = [a + b],$$

$$\cdot : \mathbb{Z}/n \times \mathbb{Z}/n \rightarrow \mathbb{Z}/n : [a] \cdot [b] = [a \cdot b].$$

Alle Axiome eines kommutativen Rings gelten in  $(\mathbb{Z}, +, 0, \cdot, 1)$ , und  $q : \mathbb{Z} \twoheadrightarrow \mathbb{Z}/n$  überträgt diese auf  $(\mathbb{Z}/n, +, [0], \cdot, [1])$ . So wird  $\mathbb{Z}/n$  zu einem kommutativen Ring und  $q$  zu einem Ringhomomorphismus.

**!** Der entscheidende Punkt der gesamten Konstruktion ist die Wohldefiniertheit der Addition und der Multiplikation auf  $\mathbb{Z}/n$ . Ab da liegen alle Daten explizit vor, und es genügt sorgsames Rechnen!

Wir nutzen die Surjektion  $q : \mathbb{Z} \twoheadrightarrow \mathbb{Z}/n$  und die Eigenschaften

$$q(a + b) = q(a) + q(b) \quad \text{und} \quad q(a \cdot b) = q(a) \cdot q(b).$$

Wir weisen für  $(\mathbb{Z}/n, +, \cdot)$  die Axiome eines kommutativen Rings nach.

Wir zeigen zunächst **Ass**( $\mathbb{Z}/n, +$ ). Vorgelegt seien  $r_1, r_2, r_3 \in \mathbb{Z}/n$ .

Hierzu existieren Urbilder  $a_1, a_2, a_3 \in \mathbb{Z}$  mit  $q(a_i) = r_i$ . Damit finden wir:

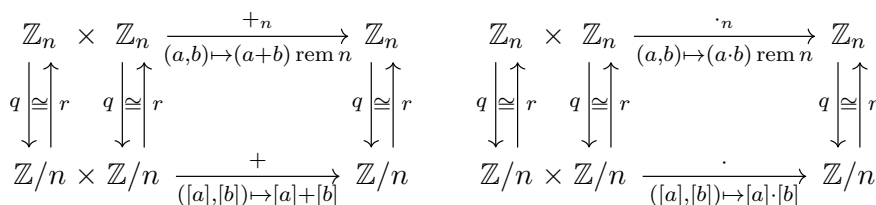
$$(r_1 + r_2) + r_3 = (q(a_1) + q(a_2)) + q(a_3) = q((a_1 + a_2) + a_3)$$

$$r_1 + (r_2 + r_3) = q(a_1) + (q(a_2) + q(a_3)) = q(a_1 + (a_2 + a_3))$$

Aus **Ass**( $\mathbb{Z}, +$ ) folgt **Ass**( $\mathbb{Z}/n, +$ ). Ebenso alle anderen Ringaxiome A1E!

**😊** Jede Allaussage in  $(\mathbb{Z}, +, \cdot)$  vererbt sich auf  $(\mathbb{Z}/n, +, \cdot)$  dank des Homomorphismus  $q : \mathbb{Z} \twoheadrightarrow \mathbb{Z}/n$ . Bitte führen Sie dies sorgsam aus!

Sei  $n \in \mathbb{N}_{\geq 1}$  und  $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$ . Wir haben das Bijektionspaar  $(q, r) : \mathbb{Z}_n \cong \mathbb{Z}/n$  mit  $q(a) = [a]$  und  $r([a]) = a \text{ rem } n$ . (Wohldefiniert!)



**😊** Beide Ringe leisten dasselbe, und  $(q, r)$  übersetzt alles verlustfrei. Somit ist  $(q, r) : (\mathbb{Z}_n, +_n, \cdot_n) \cong (\mathbb{Z}/n, +, \cdot)$  ein Ringisomorphismus.

Sie können sich daher aussuchen, wie Sie rechnen möchten:

- M** mit Restklassen  $[0], [1], \dots, [n-1]$  im Restklassenring  $\mathbb{Z}/n$  oder
- I** mit den kanonischen Repräsentanten  $0, 1, \dots, n-1$  im Ring  $\mathbb{Z}_n$ .

Restklassen sind die mathematische Sichtweise: elegant und abstrakt. Die Repräsentanten eignen sich besonders gut für die Programmierung, so können Sie alle Rechnungen direkt und effizient implementieren.

**Aufgabe:** Warum ist  $r : \mathbb{Z}/n \rightarrow \mathbb{Z}_n : [a] \mapsto a \text{ rem } n$  wohldefiniert?

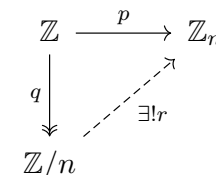
**Lösung:** Wir nutzen den Faktorisierungssatz E3J!

Die Abbildung  $p : \mathbb{Z} \rightarrow \mathbb{Z}_n : a \mapsto a \text{ rem } n$  ist kompatibel

mit  $q : \mathbb{Z} \twoheadrightarrow \mathbb{Z}/n : a \mapsto [a]$ , denn  $[a] = [b]$  bedeutet

$a - b \in n\mathbb{Z}$ , also  $a \text{ rem } n = b \text{ rem } n$ . Faktorisierung

gibt  $r : \mathbb{Z}/n \rightarrow \mathbb{Z}_n$  mit  $p = r \circ q$ , also  $r([a]) = a \text{ rem } n$ .



**😊** Der Faktorisierungssatz ist das Universalwerkzeug, um Abbildungen auf einer Quotientenmenge zu konstruieren. Nur so gelingt es!

**Aufgabe:** Warum ist  $(q, r) : \mathbb{Z}_n \cong \mathbb{Z}/n$  ein Bijektionspaar?

**Lösung:** Für jedes  $a \in \mathbb{Z}_n$  gilt  $r(q(a)) = r([a]) = a \text{ rem } n = a$ .

Umgekehrt sei  $x \in \mathbb{Z}/n$ . Also gilt  $x = [a]$  mit  $a \in \mathbb{Z}$ . Die euklidische

Division ergibt  $a = nk + a'$  mit  $k = a \text{ quo } n \in \mathbb{Z}$  und  $a' = a \text{ rem } n \in \mathbb{Z}_n$ .

Damit erhalten wir  $q(r(x)) = q(r([a])) = q(a') = [a'] = [a] = x$ .

**😊** Alle Daten liegen explizit vor, es genügt sorgsames Nachrechnen! Wir werden fortan  $\mathbb{Z}_n$  und  $\mathbb{Z}/n$  meist nicht mehr unterscheiden.

**Aufgabe:** Wir betrachten den Restklassenring  $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ .

(0) Schreiben Sie die Abbildung  $f: \mathbb{Z}_9 \rightarrow \mathbb{Z}_9: x \mapsto x^3$  explizit aus mit den kanonischen Repräsentanten  $\bar{0}, \bar{1}, \dots, \bar{8}$ . (1) Ist  $f$  injektiv? (2) surjektiv?

**Lösung:** (0) Wir rechnen sorgsam modulo 9:

$x$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{8}$
$f(x)$	$\bar{0}$	$\bar{1}$	$\bar{8}$	$\bar{0}$	$\bar{1}$	$\bar{8}$	$\bar{0}$	$\bar{1}$	$\bar{8}$

(1) In  $\mathbb{Z}_9$  gilt  $\bar{0} \neq \bar{3}$ , aber  $f(\bar{0}) = \bar{0} = f(\bar{3})$ , daher ist  $f$  nicht injektiv.

(2) Zu  $y = \bar{2}$  gibt es kein  $x \in \mathbb{Z}_9$  mit  $f(x) = y$ . Somit ist  $f$  nicht surjektiv.

**Aufgabe:** (3) Dieselben Fragen für  $g: \mathbb{Z}_{11} \rightarrow \mathbb{Z}_{11}: x \mapsto x^3$ .

(4) Wie / Können Sie  $g$  als Produkt disjunkter Zyklen schreiben?

**Lösung:** (3) Die Abbildung  $g: \mathbb{Z}_{11} \rightarrow \mathbb{Z}_{11}: x \mapsto x^3$  ist bijektiv:

$x$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{8}$	$\bar{9}$	$\bar{10}$
$g(x)$	$\bar{0}$	$\bar{1}$	$\bar{8}$	$\bar{5}$	$\bar{9}$	$\bar{4}$	$\bar{7}$	$\bar{2}$	$\bar{6}$	$\bar{3}$	$\bar{10}$

(4) Wir finden  $g = (\bar{0}) (\bar{1}) (\bar{2}, \bar{8}, \bar{6}, \bar{7}) (\bar{3}, \bar{5}, \bar{4}, \bar{9}) (\bar{10})$ .

**Aufgabe:** Auf der Menge  $\mathbb{R}$  definieren wir die Relation  $\sim$  wie folgt:

Genau dann gilt  $x \sim y$ , wenn ein  $\lambda \in \mathbb{R}_{\geq 1}$  existiert mit  $\lambda x = y$ .

(1) Welche der drei Axiome einer Äquivalenzrelation sind erfüllt?

Auf der Menge  $\mathbb{R}$  sei  $\approx$  die von  $\sim$  erzeugte Äquivalenzrelation.

(2) Explizieren Sie  $\approx$ . (3) Nennen Sie alle Äquivalenzklassen.

**Lösung:** (1) Es gilt Reflexivität und Transitivität, aber nicht Symmetrie.

(1a) Reflexivität ist erfüllt: Für jedes  $x \in \mathbb{R}$  gilt  $x \sim x$ , denn  $\lambda x = x$  mit  $\lambda = 1 \in \mathbb{R}_{\geq 1}$ .

(1b) Symmetrie ist nicht erfüllt: Zum Beispiel gilt  $3 \sim 6$ , denn  $\lambda 3 = 6$  mit  $\lambda = 2 \in \mathbb{R}_{\geq 1}$ , aber nicht  $6 \sim 3$ , denn  $1/2 \notin \mathbb{R}_{\geq 1}$ .

(1c) Transitivität ist erfüllt: Aus  $\lambda x = y$  und  $\mu y = z$  mit  $\lambda, \mu \in \mathbb{R}_{\geq 1}$  folgt  $\kappa x = z$  mit  $\kappa = \mu\lambda \in \mathbb{R}_{\geq 1}$ .

(2) Genau dann gilt  $x \approx y$ , wenn ein  $\lambda \in \mathbb{R}_{>0}$  existiert mit  $\lambda x = y$ .

(Ausführung als Übung: Beweisen Sie diese explizite Darstellung!)

(3) Die Zerlegung in Äquivalenzklassen ist  $\mathbb{R}/\approx = \{\mathbb{R}_{<0}, \{0\}, \mathbb{R}_{>0}\}$ .

**Aufgabe:** Auf der Menge  $\mathbb{R}$  definieren wir die Relation  $\sim$  wie folgt:

Genau dann gilt  $x \sim y$ , wenn ein  $\lambda \in [\frac{1}{2}, 2]$  existiert mit  $\lambda x = y$ .

(1) Welche der drei Axiome einer Äquivalenzrelation sind erfüllt?

Auf der Menge  $\mathbb{R}$  sei  $\approx$  die von  $\sim$  erzeugte Äquivalenzrelation.

(2) Explizieren Sie  $\approx$ . (3) Nennen Sie alle Äquivalenzklassen.

**Lösung:** (1) Es gilt Reflexivität und Symmetrie, aber nicht Transitivität.

(1a) Reflexivität ist erfüllt: Für jedes  $x \in \mathbb{R}$  gilt  $x \sim x$ , denn  $\lambda x = x$  mit  $\lambda = 1 \in [\frac{1}{2}, 2]$ . (1b) Symmetrie ist erfüllt: Ist  $x \sim y$ , dann ist  $\lambda x = y$  mit  $\lambda \in [\frac{1}{2}, 2]$ , also  $\lambda^{-1}y = x$ . Dank  $\lambda^{-1} \in [\frac{1}{2}, 2]$  folgt  $y \sim x$ . (1c) Transitivität ist nicht erfüllt: Zum Beispiel gilt  $1 \sim 2$  und  $2 \sim 4$ , aber  $1 \not\sim 4$ .

(Zur Übung können Sie diese Aufgabe vielfältig variieren:

Beginnen Sie mit  $\lambda \in S = \mathbb{R}_{\geq 1}, \mathbb{R}_{>1}, [\frac{1}{2}, 2], [1, 2], [2, 3], \dots$ )

(2) Genau dann gilt  $x \approx y$ , wenn ein  $\mu \in \mathbb{R}_{>0}$  existiert mit  $\mu x = y$ .

(Ausführung als Übung: Beweisen Sie diese explizite Darstellung!)

(3) Die Zerlegung in Äquivalenzklassen ist  $\mathbb{R}/\approx = \{\mathbb{R}_{<0}, \{0\}, \mathbb{R}_{>0}\}$ .

**Ausführung:** Auf der Menge  $\mathbb{R}$  definieren wir die Relation  $\simeq$  wie folgt:

Genau dann gilt  $x \simeq y$ , wenn ein  $\mu \in \mathbb{R}_{>0}$  existiert mit  $\mu x = y$ .

Diese Relation findet man anschaulich durch transitive Fortsetzung.

Wir zeigen nun, dass  $\simeq$  gleich  $\approx$  ist, wie oben in (2) behauptet.

(2a) Zunächst prüfen wir nach, dass  $\simeq$  eine Äquivalenzrelation ist.

Wie oben in (1) ist dies leichte Routine. (1a) Reflexivität: Für jedes  $x \in \mathbb{R}$  gilt  $x \simeq x$ , denn  $\lambda x = x$  mit  $\lambda = 1 \in \mathbb{R}_{>0}$ . (1b) Symmetrie: Ist  $x \sim y$ , dann ist  $\lambda x = y$  mit  $\lambda \in \mathbb{R}_{>0}$ , also  $\lambda^{-1}y = x$ . Dank  $\lambda^{-1} \in \mathbb{R}_{>0}$  folgt  $y \sim x$ .

(1c) Transitivität: Aus  $\lambda x = y$  und  $\mu y = z$  mit  $\lambda, \mu \in \mathbb{R}_{>0}$  folgt  $\kappa x = z$  mit  $\kappa = \mu\lambda \in \mathbb{R}_{>0}$ .

(2b) Offensichtlich gilt  $x \sim y \Rightarrow x \simeq y$ , das heißt  $\simeq$  enthält  $\sim$ .

Dank (2a) enthält  $\simeq$  die von  $\sim$  erzeugte Äquivalenzrelation  $\approx$ .

(2c) Umgekehrt zeigen wir schließlich:  $\approx$  enthält  $\simeq$ , also  $x \simeq y \Rightarrow x \approx y$ .

Angenommen, es gilt  $x \simeq y$ , also  $\mu x = y$  mit  $\mu \in \mathbb{R}_{>0}$ . Wir können dann ein  $n \in \mathbb{N}$  so wählen, dass  $\kappa := \sqrt[n]{\mu} \in [\frac{1}{2}, 2]$ . Für  $i = 0, \dots, n$  setzen wir

$x_i = \kappa^i x$ . Dann ist  $x = x_0 \sim x_1 \sim \dots \sim x_n = y$ , also  $x \approx y$ .

## Wie un/wahrscheinlich sind lange Zyklen?

E353  
Übung

**Aufgabe:** (1) Vorgelegt seien  $n, \ell \in \mathbb{N}$  mit  $n/2 < \ell \leq n$ .  
Wie viele Permutationen  $\sigma \in S_n$  haben einen  $\ell$ -Zykel?

**Lösung:** (1) Hat  $\sigma \in S_n$  einen  $\ell$ -Zykel, so sind alle anderen Zyklen strikt kürzer, denn  $\ell > n/2$ . Zur Konstruktion von  $\sigma$  wählen wir zunächst die Elemente des  $\ell$ -Zykels: Dazu gibt es  $\binom{n}{\ell}$  Möglichkeiten, diese können wir auf  $\ell!$  Weisen anordnen, je  $\ell$  Anordnungen ergeben denselben Zykel. Die verbleibenden  $n - \ell$  Punkte können wir beliebig permutieren. Die gesuchte Anzahl ist demnach

$$a_\ell = \binom{n}{\ell} \cdot \ell! \cdot (n - \ell)! = \frac{n!}{\ell}.$$

😊 Das ist eine erfreulich einfache Formel!

**Beispiel:** Wir betrachten Permutationen von  $n = 10$  Punkten. Der Anteil der Permutationen mit einem  $\ell$ -Zykel ist genau  $1/\ell$  für  $\ell = 6, 7, \dots, 10$ .  
Spezialfall: 10% dieser Permutationen bestehen aus einem 10-Zykel. Diesen Fall können Sie besonders leicht erklären. Versuchen Sie es!

## Wie un/wahrscheinlich sind lange Zyklen?

E354  
Übung

**Aufgabe:** (2) Sei  $n = 2m$ . Sie wählen zufällig eine Permutation  $\sigma \in S_n$ .  
Wie wahrscheinlich sind Permutationen mit einem Zykel der Länge  $> m$ ?

**Lösung:** (2) Dank der vorigen Aufgabe ist die Wahrscheinlichkeit

$$p_n = \frac{1}{n!} \sum_{\ell=m+1}^n \frac{n!}{\ell} = \sum_{\ell=m+1}^n \frac{1}{\ell}.$$

Für  $n = 2, 4, 6, 8, 10, \dots$  erhalten wir folgende numerische Werte:

$n$	2	4	6	8	10	20	50	100	200	500
$p_n$	0.500	0.583	0.617	0.635	0.646	0.669	0.683	0.688	0.691	0.692
$1 - p_n$	0.500	0.417	0.383	0.365	0.354	0.331	0.317	0.312	0.309	0.308

😊 Für große  $n$  nutzen wir geschickt den Vergleich mit dem Integral:

$$\ln \left( 2 - \frac{1}{m+1} \right) = \int_{x=m}^{2m} \frac{1}{x+1} dx \leq \sum_{\ell=m+1}^{2m} \frac{1}{\ell} \leq \int_{x=m}^{2m} \frac{1}{x} dx = \ln 2$$

Somit gilt  $p_n \nearrow \ln 2 \approx 0.693$  und  $1 - p_n \searrow 1 - \ln 2 \approx 0.307$ .

## Das Erstirätsel (aka Gefangenenrätsel)

E355  
Übung

Zur Erstsemestereinführung veranstaltet die Fachschaft folgendes Spiel. In einem Team von  $n = 10$  Erstis trägt jeder eine Nummer  $1, 2, \dots, n$ . Sie betreten nacheinander einen Raum mit  $n$  Boxen, diese enthalten zufällig verteilt die Zahlen  $1, 2, \dots, n$ . Jeder Ersti muss seine Nummer finden und darf dazu in  $n/2 = 5$  Boxen schauen; danach verlässt er den Raum durch eine andere Tür. Findet jeder Ersti seine eigene Nummer, so gewinnt das Team. Findet aber irgendein Ersti seine Nummer nicht, so verliert das Team. Vor dem Spiel darf das Team sich beraten, doch während des Spiels ist keine Kommunikation mehr möglich.

**Aufgabe:** (3) Angenommen, jeder Ersti öffnet seine Boxen zufällig. Welche Gewinnwkt hat das Team mit dieser Zufallsstrategie?

(4) Gibt es eine Strategie mit Gewinnwkt über 30%?  
Was ist für das Team die beste Strategie?

**Lösung:** (3) Bei zufälligem Öffnen hat jeder Ersti die Gewinnwkt  $\frac{1}{2}$ , das Team also die Gewinnwkt  $\frac{1}{2^n}$ . Für  $n = 10$  ist dies  $\frac{1}{1024} \approx 0.1\%$ .

## Das Erstirätsel (aka Gefangenenrätsel)

E356  
Übung

(4) Jeder Ersti  $k = 1, 2, \dots, n$  spielt die **Zykelverfolgungs-Strategie**: Er schaut zuerst in die Box mit seiner Nummer  $i_1 = k$ ; liegt dort die Nummer  $k$ , so hat er gewonnen. Andernfalls sieht er dort die Nummer  $i_2 \neq i_1$  und öffnet die Box Nummer  $i_2$ . Dies wiederholt er solange, bis er seine Nummer gefunden hat (oder aufhören muss).

Die Verteilung der Nummern auf die Boxen entspricht einer Permutation  $\sigma \in S_n$ . Das Team verliert mit dieser Strategie, falls ein Zykel der Länge  $> n/2$  vorliegt. Die Wkt hierfür ist  $p_{10} = \sum_{\ell=6}^{10} \frac{1}{\ell} \approx 0.646$  wie oben in (2) berechnet. Das Team gewinnt also mit der Wkt  $1 - p_{10} \approx 0.354$ .

😊 Für  $n \rightarrow \infty$  konvergiert die Wkt  $\frac{1}{2^n}$  in (1) sehr schnell gegen 0, während die Wkt  $1 - p_n \searrow 1 - \ln 2 \approx 0.307$  immer über 30% bleibt.

😊 Die Zykelverfolgungs-Strategie ist tatsächlich optimal, das heißt sie maximiert die Gewinnwkt. Dies bewiesen E. Curtin, M. Warshauer: *The locker puzzle*. Mathematical Intelligencer 28 (2006) 28–31.

Siehe [en.wikipedia.org/wiki/100\\_prisoners\\_problem](http://en.wikipedia.org/wiki/100_prisoners_problem).