Skript: Lineare Algebra I

Prof. Dr. Vladimir Lazić

(nach dem Mitschrieb von Niklas Schneider im Wintersemester 2019/20)

Inhaltsverzeichnis

1 Mengen und Abbildungen

Definition 1.1. Eine **Menge** M ist eine Ansammlung wohlbestimmter Objekte.

Beispiel 1.2.

(1) Die Menge aller Buchstaben im englischen Alphabet:

$$A := \{A, a, B, b, \ldots, Z, z\}.$$

(Hier sprechen wir „:=“ aus als „ist definiert durch“.)

(2) Die Menge aller Hörer dieser Vorlesung:

$$B := \{\text{alle Hörer dieser Vorlesung}\}.$$

(3) Alle Primzahlen, die kleiner als zehn sind:

$$C := \{2, 3, 5, 7\}.$$

Bemerkung 1.3.

(1) Die Reihenfolge der Elemente spielt keine Rolle:

$$C = \{3, 2, 7, 5\} = \{2, 7, 5, 3\}.$$

(2) Die Objekte einer Menge M nennt man *Elemente von M.*

Beispiel 1.4. Wir haben die folgenden speziellen Mengen:

(1) Die *leere Menge* $\{\} = \emptyset$.

(2) Die *natürlichen Zahlen* $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$.

(3) Die *ganzen Zahlen* $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \ldots\}$.

(4) Die *reellen Zahlen* $\mathbb{R} = \{\text{unendliche Dezimalzahlen}\}$.

(5) Die *komplexen Zahlen* $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$.

Bemerkung 1.5.

(1) Wenn ein Element a zu einer Menge A gehört, dann schreiben wir

$$a \in A \quad \text{oder} \quad A \ni a.$$

(2) Wenn a nicht zu einer Menge A gehört, dann schreiben wir

$$a \notin A \quad \text{oder} \quad A \not\ni a.$$

(3) Seien M und N zwei Mengen. Wenn jedes Element von N auch ein Element von M ist, dann sagen wir, dass N eine *Untermenge* oder *Teilmenge von* M ist und schreiben

$$N \subset M \quad \text{oder} \quad N \subseteq M.$$

(4) Eine Teilmenge $N \subseteq M$ heißt *echte Teilmenge*, wenn $N \neq \emptyset$ und $N \neq M$. Dann schreiben wir auch

$$N \subsetneq M.$$

(5) Wenn N keine Teilmenge von M ist, so schreiben wir

$$N \not\subseteq M.$$

Definition 1.6. Sei M eine Menge. Die Anzahl von Elementen von M bezeichnen wir mit

$$|M| \quad \text{oder} \quad \#M.$$

Diese Zahl heißt *Kardinalität* oder *Mächtigkeit* von M.

Beispiel 1.7.

(1) $|\emptyset| = 0$

(2) $|\{\text{Buchstaben des englischen Alphabets}\}| = 26$

(3) $|\{0\}| = 1$

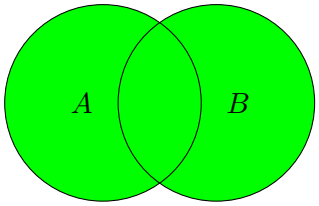
(4) Hat M unendlich viele Elemente, so schreiben wir $|M| = \infty$.

Definition 1.8. Seien A und B Mengen. Dann ist die *Vereinigung* von A und B die Menge

$$A \cup B := \{x \in A \text{ oder } x \in B\}.$$

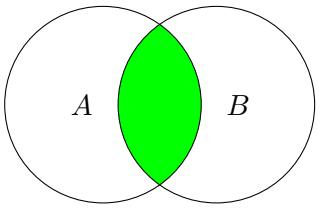
Für Mathematiker bedeutet „oder“ *nicht* „exklusiv oder“, d.h. es gilt:

$$A \cup B = \{x \text{ gehört zu } A, \text{ zu } B \text{ oder zu den beiden Mengen}\}.$$



Der *Durchschnitt* von A und B ist die Menge

$$A \cap B := \{x \in A \text{ und } x \in B\}.$$

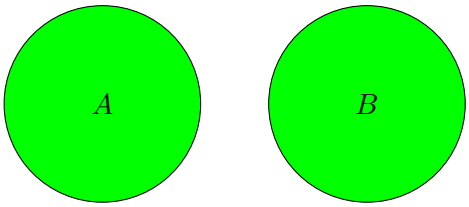


Gilt $A \cap B = \emptyset$, dann sind A und B *disjunkt*. Dann schreiben wir für $A \cup B$ auch

$$A \sqcup B,$$

und nennen diese Vereinigung *disjunkt*. Für eine disjunkte Vereinigung gilt

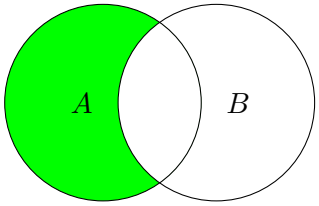
$$|A \sqcup B| = |A| + |B|.$$



Die *Differenz* von A und B ist die Menge

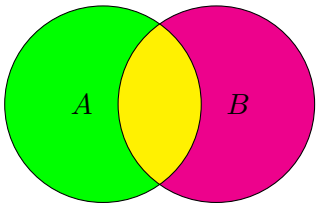
$$A \setminus B := \{x \mid x \in A \text{ und } x \notin B\}.$$

Wir sprechen dies aus als „A minus B“ und schreiben manchmal auch $A - B$.



Damit lässt sich die Vereinigung ausdrücken als

$$A \cup B = (A \setminus B) \sqcup (A \cap B) \sqcup (B \setminus A).$$



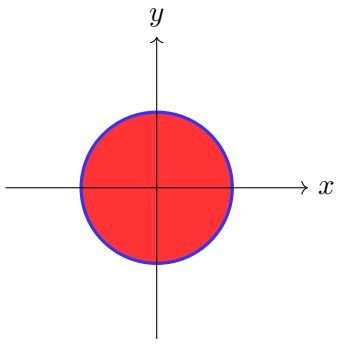
Beispiel 1.9. Betrachte die folgenden Mengen:

(1) $\delta_1 = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 \leq 1\}$,

(2) $\delta_2 = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\}$,

(3) $\delta_3 = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 < 1\}$.

Dann gilt $\delta_1 = \delta_2 \sqcup \delta_3$.



Lemma 1.10. *Seien A, B und C Mengen. Dann gelten die* Distributivgesetze*:*

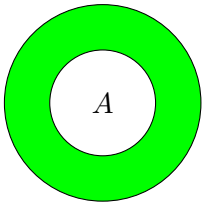
(1) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$,

(2) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Definition 1.11. Betrachte eine Menge A, die Teilmenge einer bestimmten Menge M ist. Dann schreiben wir

$$\overline{A}$$

für die Menge $M \setminus A$. Dies sprechen wir aus als „A Komplement“ und schreiben auch A^c.



Lemma 1.12. *Seien A und B Teilmengen einer Menge M. Dann gelten die* Gesetze von De Morgan*:*

$$\overline{A \cup B} = \overline{A} \cap \overline{B}, \quad \overline{A \cap B} = \overline{A} \cup \overline{B}, \quad \overline{\overline{A}} = A.$$

Definition 1.13. Seien A und B Mengen. Dann bezeichnet

$$\begin{aligned} A \times B :&= \{(a,b) \mid a \in A,\, b \in B\} \\ &= \{\text{alle geordneten Paare } (a,b) \text{ mit } a \in A,\, b \in B\} \end{aligned}$$

das *(kartesische) Produkt von A und B.*

Bemerkung 1.14. Wenn $A = B$ in der obigen Definition, dann schreiben wir auch

$$A^2 := A \times A,$$

und in ähnlicher Weise:

$$A^n := \underbrace{A \times A \times \cdots \times A}_{n \text{ mal}}.$$

Beispiel 1.15. $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R} = \{(a,b) \mid a, b \in \mathbb{R}\}$.

Bemerkung 1.16. Probleme mit der Definition einer Menge:

(1) Sei L die Liste aller Sachen, die ich in meiner Tasche habe, zum Beispiel

$$L = \{\text{Kulis, Papier, Taschentücher}\}.$$

Wenn ich nun L in meine Tasche stecke, dann enthält die Tasche die Liste L, das heißt

$$L = \{\text{Kulis, Papier, Taschentücher, } L\}.$$

Das heißt, nach unserer Definition können Mengen sich selbst enthalten.

(2) *Russelsche Antimonie*
Sei M die Menge aller Mengen, die sich selbst nicht enthalten. Frage: Ist $M \in M$?
Wenn $M \in M$, dann gilt $M \notin M$ nach Definition von M. Wenn $M \notin M$, dann gilt $M \in M$ nach Definition von M. Fazit: M ist keine Menge. In der Mengenlehre löst man dieses Problem, indem man den Begriff *Familie* einführt.

Definition 1.17. Die Menge aller Teilmengen einer Menge M nennt man die *Potenzmenge von* M, und schreibt

$$\mathcal{P}(M).$$

Satz 1.18. *Sei M eine endliche Menge. Dann gilt*

$$|\mathcal{P}(M)| = 2^{|M|}.$$

Beweis. Übung! □

Funktionen

Definition 1.19. Seien M und N zwei Mengen. Eine *Abbildung* oder eine *Funktion* zwischen M und N ordnet *jedem* Element in M *genau ein* Element aus N zu. Wenn wir eine Zuordnung durch f bezeichnen, dann schreiben wir

$$f\colon M \to N, \quad x \mapsto f(x).$$

Hier heißt M *die Urmenge* und N *die Zielmenge* von f. Die Menge aller Abbildungen von M nach N bezeichnen wir mit $\mathrm{Abb}(M, N)$.

Beispiel 1.20. Seien $M = \{a, b, c, d\}$ und $N = \{1, 3\}$. Eine Funktion von M nach N können wir beispielsweise durch Zuordnung von Elementen definieren:

$$(a \mapsto 3,\ b \mapsto 3,\ c \mapsto 1,\ d \mapsto 3).$$

Eine Funktion kann auch durch eine Formel gegeben werden:

$$f\colon \mathbb{R} \to \mathbb{R}, \quad x \mapsto x^2 + 1.$$

Notation 1.21. Sei M eine Menge. Die Abbildung

$$\mathrm{id}_M\colon M \to M, \quad m \to m$$

heißt die *Identität auf* M.

Bemerkung 1.22. Eine Funktion $f\colon M \to N$ heißt *wohldefiniert*, falls für jedes $m \in M$ gilt $f(m) \in N$ und für jedes $M \in M$ genau ein $n \in N$ existiert, sodass $n = f(m)$.

Beispiel 1.23. Es gibt keine Funktion $f\colon \mathbb{R} \to \mathbb{N}$ mit $f(x) = x^2 + 1$, da $f\left(\frac{5}{2}\right) \notin \mathbb{N}$.

Definition 1.24. Sei $f\colon M \to N$ eine Funktion und $A \subseteq M$ eine Teilmenge von M. Dann heißt die Menge

$$f(A) := \left\{x \in N \mid \exists\, y \in A \text{ mit } x = f(y)\right\} = \{f(x) \mid x \in A\}$$

das *Bild von* A.[1] Für eine Teilmenge $B \subseteq N$ heißt die Menge

$$f^{-1}(B) := \{x \in M \mid f(x) \in B\}$$

das *Urbild von* B. Für eine einelementige Teilmenge $\{y\} \subseteq N$ schreiben wir auch $f^{-1}(y)$ statt $f^{-1}(\{y\})$, und nennen wir die Menge $f^{-1}(y)$ die *Faser von* f *über* y.

Beispiel 1.25. Im Beispiel 1.20 gilt:

$$f(M) = \{1, 3\}, \qquad f^{-1}(1) = \{c\}, \qquad f^{-1}(3) = \{a, b, d\}.$$

Definition 1.26. Sei $f\colon M \to N$ eine Abbildung und sei $A \subseteq M$ eine Teilmenge von M. Wir bezeichnen mit

$$f\,|_A\colon A \to N$$

(und lesen „f eingeschränkt auf A“) die Abbildung

$$A \ni x \mapsto f(x) \in N.$$

Definition 1.27. Sei $f\colon M \to N$ eine Abbildung. Die Menge

$$\Gamma_f \subseteq M \times N$$

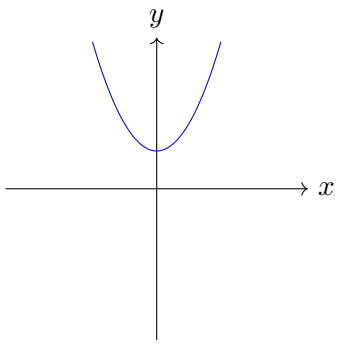
gegeben durch

$$\Gamma_f := \{(x, y) \in M \times N \mid y = f(x)\} = \{(x, f(x)) \mid x \in M\}$$

ist der *Graph von* f.

[1] Wir benutzen zwei *Quantoren*: $\forall$ = „für alle“ und $\exists$ = „es existiert“.

Beispiel 1.28. Der Graph von $f\colon \mathbb{R} \to \mathbb{R},\ x \mapsto x^2 + 1$ ist



Definition 1.29. Sei $f\colon M \to N$ eine Abbildung. Dann heißt f:

(1) *injektiv*, falls für alle $x, y \in M$ mit $x \neq y$ gilt $f(x) \neq f(y)$;

(2) *surjektiv*, falls für jedes $n \in N$ ein $m \in M$ existiert, sodass $f(m) = n$;

(3) *bijektiv*, falls f surjektiv und injektiv ist.

Eine unendliche Menge M heißt *abzählbar*, falls es eine bijektive Abbildung $f\colon \mathbb{N} \to M$ gibt; ansonsten heißt M *überabzählbar*.

Beispiel 1.30. Im Beispiel 1.20 ist die Abbildung f weder injektiv noch surjektiv, da $f^{-1}(3) = \{a, b, d\}$ und $f(M) = \{1, 3\}$.

Lemma 1.31. *Die Menge* $\mathbb{R}$ *ist überabzählbar.*

Beweis. Angenommen, es existiert eine bijektive Abbildung $f\colon \mathbb{N} \to \mathbb{R}$. Wir werden einen Widerspruch herleiten. Die Abbildung f lässt sich darstellen als

$$\begin{aligned} f(0) &= n_0, d_{0,1}d_{0,2}d_{0,3}\dots \\ f(1) &= n_1, d_{1,1}d_{1,2}d_{1,3}\dots \\ f(2) &= n_2, d_{2,1}d_{2,2}d_{2,3}\dots \\ f(3) &= n_3, d_{3,1}d_{3,2}d_{3,3}\dots \\ &\dots \end{aligned}$$

wobei für alle $i, j \in \mathbb{N}$ wir haben $n_j \in \mathbb{Z}$ und $d_{j,i} \in \{0, 1, 2, \dots, 9\}$. Für jedes $i \in \mathbb{N}$ setze

$$r_i := \begin{cases} r_i = 5, & \text{falls } d_{i,i} = 4, \\ 4, & \text{sonst}, \end{cases}$$

und definiere

$$r := 0, r_1 r_2 r_3 \dots$$

Dann ist r eine reelle Zahl, die nicht in der obigen Liste steht, denn r unterscheidet sich von $f(i)$ an der i-ten Stelle nach dem Komma, für jedes $i \in \mathbb{N}$. Das ist ein Widerspruch. □

Bemerkung 1.32. Ein mögliches Problem im obigen Beweis: Eine reelle Zahl kann zwei unterschiedliche Darstellungen haben, zum Beispiel $0,945\overline{9} = 0,946$. Aber dies ist auch die einzige Möglichkeit, also wenn *fast alle Ziffern gleich* 9 *sind*. Im obigen Beweis tritt dieses Problem nicht auf, da r per Konstruktion nur aus 4 und 5 besteht.

Notation 1.33. Sei I eine Indexmenge, und für jedes $i \in I$ sei A_i eine Menge. Setze:

$$\bigcup_{i \in I} A_i := \{x \mid \exists i \in I \text{ mit } x \in A_i\},$$
$$\bigcap_{i \in I} A_i := \{x \mid \forall i \in I \text{ gilt } x \in A_i\}.$$

Satz 1.34. *Sei $f\colon M \to N$ eine Abbildung zwischen endlichen Mengen M und N mit $|M| = |N|$. Dann sind äquivalent:*

(a) f ist injektiv,

(b) f ist surjektiv,

(c) f ist bijektiv.

Beweis. Die Implikationen $(c) \Rightarrow (a)$ und $(c) \Rightarrow (b)$ folgen aus der Definition.

$(a) \Rightarrow (b)$: Sei f injektiv. Für alle $n_1, n_2 \in \mathbb{N}$ mit $n_1 \neq n_2$, die Mengen $f^{-1}(n_1)$ und $f^{-1}(n_2)$ sind disjunkte Teilmengen von M (per Definition einer Funktion); und in ähnlicher Weise gilt $\bigcup_{n \in N} f^{-1}(n) = M$. Daraus folgt:

$$M = \bigsqcup_{n \in N} f^{-1}(n).$$

Damit gilt

$$|M| = \sum_{n \in N} |f^{-1}(n)|,$$

und deswegen:

$$|M| = \sum_{n \in N} \underbrace{|f^{-1}(n)|}_{\leq 1} \overset{f \text{ inj.}}{\leq} \sum_{n \in N} 1 = |N|.$$

Aber wir wissen, dass $|M| = |N|$, und damit $\sum_{n\in N} |f^{-1}(n)| = \sum_{n\in N} 1$. Die impliziert $|f^{-1}(n)| = 1$ für alle $n \in N$, und damit ist f surjektiv.

$(a) \Leftarrow (b)$: Sei f surjektiv. Ähnlich wie oben haben wir:

$$|M| = \sum_{n\in N} \underbrace{|f^{-1}(n)|}_{\geq 0} \overset{f \text{ sur.}}{\geq} \sum_{n\in N} 1 = |N|.$$

Aber wir wissen, dass $|M| = |N|$, und damit $\sum_{n\in N} |f^{-1}(n)| = \sum_{n\in N} 1$. Dies impliziert $|f^{-1}(n)| = 1$ für alle $n \in N$, und damit ist f injektiv.

Dies zeigt $(a) \Leftrightarrow (b)$, und somit sind die fehlenden Implikationen bewiesen. □

Korollar 1.35. *Seien M und N endliche Mengen. Ist $f\colon M \to N$ eine injektive Abbildung, so gilt*

$$|M| \leq |N|.$$

Ist f eine surjektive Abbildung, so gilt

$$|M| \geq |N|.$$

Ist f eine bijektive Abbildung, so gilt

$$|M| = |N|.$$

Beweis. Folgt aus dem Beweis von Satz 1.34. □

Korollar 1.36 (Schubfachprinzip)**.** *Eine Abbildung $f\colon M \to N$ mit $|M| > |N|$ ist nicht injektiv.*

Beweis. Das ist die Kontraposition zum obigen Korollar. □

Beispiel 1.37. Gegeben seien $n^2 + 1$ Punkte im folgenden $n \times n$ Quadrat:

$$Q = \{(x, y) \in \mathbb{R}^2 \mid 0 \leq x, y \leq n\}.$$

Dann existieren zwei Punkte $a, b \in Q$, sodass der Abstand zwischen a und b kleiner oder gleich $\sqrt{2}$ ist.

Beweis. Wir unterteilen Q in n^2 Einheitsquadrate. Diese bezeichnen wir mit $Q_{i,j}$, wobei $1 \leq i, j \leq n$. Die $n^2 + 1$ Punkte bezeichnen wir mit P_i, wobei $1 \leq i \leq n^2 + 1$. Wir definieren eine Abbildung

$$f\colon \{1, 2, \ldots, n^2 + 1\} \to \{Q_{i,j} \mid 1 \leq i, j \leq n\}$$

wie folgt: Sei $k \in \{1, 2, \ldots, n^2 + 1\}$. Dann:

(a) falls es nur ein Quadrat $Q_{i,j}$ gibt, zu welchem der Punkt P_k gehört, dann setzen wir $f(k) := Q_{i,j}$,

(b) falls es mehrere Quadrate gibt, zu welchem der Punkt P_k gehört, dann wählen wir das Quadrat $f(k)$ so, dass es am linkesten und am untersten liegt.

Da

$$|\{1, 2, \ldots, n^2 + 1\}| = n^2 + 1 \quad \text{und} \quad |\{Q_{i,j} \mid 1 \leq i, j \leq n\}| = n^2,$$

so gibt es nach dem Schubfachprinzip zwei Werte $p, q \in \{1, 2, \ldots, n^2 + 1\}$, sodass $f(p) = f(q)$. In anderen Worten, die Punkte P_p und P_q liegen im selben Einheitsquadrat. Das impliziert, dass der Abstand zwischen P_p und P_q kleiner oder gleich der Länge der Diagonalen des Quadrats ist, also $\leq \sqrt{2}$. □

Definition 1.38. Sei $f\colon M \to N$ eine bijektive Abbildung. Die Funktion

$$f^{-1}\colon N \to M, \quad n \mapsto m,$$

wobei m das eindeutige Element in M ist, für welches $f(m) = n$ gilt, heißt die *Umkehrfunktion* zu der Funktion f.

Definition 1.39. Seien $f\colon A \to B$ und $g\colon B \to C$ zwei Abbildungen. Die Funktion

$$g \circ f\colon A \to C, a \mapsto g(f(a))$$

(ausgesprochen „g nach f“) heißt die *Komposition* oder die *Verknüpfung* von f und g.

Proposition 1.40. *Seien $f\colon A \to B$ und $g\colon B \to C$ zwei Abbildungen. Dann gilt:*

(1) $g \circ f$ injektiv $\Longrightarrow$ f injektiv,

(2) $g \circ f$ surjektiv $\Longrightarrow$ g surjektiv.

Beweis.
(1) Seien $a_1, a_2 \in A$ mit $f(a_1) = f(a_2)$. Dann gilt

$$(g \circ f)(a_1) = g(f(a_1)) = g(f(a_2)) = (g \circ f)(a_2).$$

Da $g \circ f$ injektiv ist, so folgt $a_1 = a_2$, und daher ist f injektiv.

(2) Sei $c \in C$. Da $g \circ f$ surjektiv ist, so existiert ein $a \in A$ mit $(g \circ f)(a) = c$, und damit $g(f(a)) = c$. Definiere $b := f(a)$. Dann gilt $g(b) = c$, und deswegen ist g surjektiv. □

Relationen

Definition 1.41. Seien A und B Mengen. Eine *Relation R zwischen A und B* ist eine Teilmenge von $A \times B$. Wenn $(a, b) \in R$, dann schreiben wir

$$a \, R \, b$$

(ausgesprochen: „a ist in der Relation R zu b“). Die Menge A ist die *Quellmenge* oder der *Vorbereich* von R. Die Menge B ist die *Zielmenge* oder der *Nachbereich* von R.

Beispiel 1.42. Sei $A = \{\text{Barack, Michelle}\} = B$. Betrachten wir die folgende Relation R in $A \times B$:

$$\forall (a, b) \in A \times B : \quad a \, R \, b \iff a \text{ und } b \text{ sind verheiratet.}$$

Dann gilt: Barack R Michelle, aber Barack $\not R$ Barack.

Definition 1.43. Wenn in der obigen Definition $A = B$ (also die Ziel- und die Quellmenge sind gleich), dann heißt die Relation R *homogen*, und wir sprechen über eine *Relation auf der Menge A*. Homogene Relationen bezeichnen wir normalerweise mit $\sim$.

Eine homogene Relation $\sim$ ist:

(1) *reflexiv*, wenn $a \sim a$ für alle $a \in A$,

(2) *symmetrisch*, wenn aus $a \sim b$ folgt $b \sim a$ für alle $a, b \in A$,

(3) *transitiv*, wenn aus $a \sim b$ und $b \sim c$ folgt, dass $a \sim c$ für alle $a, b, c \in A$,

(4) *antisymmetrisch*, wenn aus $a \sim b$ und $b \sim a$ folgt, dass $a = b$ für alle $a, b \in A$,

(5) eine *Äquivalenzrelation*, wenn $\sim$ reflexiv, symmetrisch und transitiv ist.

Beispiel 1.44. Betrachte die folgenden Relationen $\sim$ auf $\mathbb{N}$:

$x \sim y$	reflexiv	symmetrisch	antisymmetrisch	transitiv
$x \leq y$	ja	nein	ja	ja
x teilt y	ja	nein	ja	ja
$x + y = 7$	nein	ja	nein	nein

Definition 1.45.

(1) Seien $a, b \in \mathbb{Z}$. Wir sagen, dass die Zahl a die Zahl b *teilt* und schreiben

$$a \mid b,$$

falls es ein $k \in \mathbb{Z}$ gibt, sodass $a = nk$.

(2) Sei $n \in \mathbb{N}$. Zwei Zahlen $a, b \in \mathbb{Z}$ heißen *kongruent modulo* n, und wir schreiben

$$a \equiv b \pmod{n},$$

falls $n \mid a - b$.

Proposition 1.46. *Sei $n \in \mathbb{N}$. Dann definiert*

$$a \sim b \quad \Longleftrightarrow \quad a \equiv b \pmod{n}$$

eine Äquivalenzrelation $\sim$ auf $\mathbb{Z}$.

Beweis.
Reflexivität: Es gilt $a \sim a$ für alle $a \in \mathbb{Z}$, weil $n \mid \underbrace{a - a}_{=0}$.
Symmetrie: Sei $a \sim b$ für $a, b \in \mathbb{Z}$. Dann gilt $n \mid a - b$, und damit $n \mid b - a$, also $b \sim a$.
Transitivität: Seien $a \sim b$ und $b \sim c$ für $a, b, c \in \mathbb{Z}$. Dann existieren $k, \ell \in \mathbb{Z}$, sodass $a - b = nk$ und $b - c = n\ell$, und damit:

$$a - c = (a - b) + (b - c) = nk + n\ell = n(k + \ell).$$

Es gilt also $n \mid a - c$, und damit $a \sim c$. □

Definition 1.47. Sei M eine Menge, sei $\sim$ eine Äquivalenzrelation auf M und sei $m \in M$. Die Teilmenge

$$[m] := \{x \in M \mid x \sim m\} \subseteq M$$

heißt die *Äquivalenzklasse von m unter der Relation $\sim$ auf M*. Manchmal bezeichnen wir diese Äquivalenzklasse auch mit $\overline{m}$. Wir bezeichnen mit

$$M/\sim$$

die Menge aller Äquivalenzklassen von $\sim$ auf M (ausgesprochen: „M modulo $\sim$“).

Satz 1.48. *Sei $\sim$ eine Äquivalenzrelation auf einer Menge M. Dann bilden die Äquivalenzklassen eine* Partition *von M, das heißt*

(1) für alle $x, y \in M$ gilt entweder $[x] = [y]$ oder $[x] \cap [y] = \emptyset$, und

(2) $\bigcup_{x \in M} [x] = M$.

Beweis.
(1) Angenommen, $[x] \cap [y] \neq \emptyset$. Dann müssen wir zeigen, dass $[x] = [y]$.

Fixiere ein z aus $[x] \cap [y]$. Sei $a \in [x]$ ein beliebiges Element. Dann gilt $a \sim x$ und $x \sim z$, und damit folgt aus der Transitivität, dass

$$a \sim z.$$

Außerdem folgt aus $z \in [y]$, dass $z \sim y$. Damit folgt wieder aus der Transitivität, dass $a \sim y$; also $a \in [y]$. Dies zeigt, dass

$$[x] \subseteq [y].$$

In ähnlicher Weise zeigen wir, dass $[y] \subseteq [x]$, und damit $[x] = [y]$.

(2) Für alle $x \in M$ gilt $x \in [x]$ (Reflexivität), und somit

$$M \supseteq \bigcup_{x \in M} [x] \supseteq \bigcup_{x \in M} \{x\} = M.$$

Dies zeigt die gewünschte Gleichheit. □

Beispiel 1.49.

(1) Eine Uhr ist ein Beispiel für eine Äquivalenzrelation auf $\mathbb{Z}$, und zwar, die Relation ist $\equiv \pmod{12}$.

(2) Sei $n \in \mathbb{N}$. Die Äquivalenzklassen der Relation $\equiv \pmod{n}$ auf $\mathbb{Z}$ sind

$$[0], [1], [2], \ldots, [n-1].$$

Und zwar, die Division mit Rest besagt, dass für jedes $a \in \mathbb{Z}$ eindeutige Zahlen $q \in \mathbb{Z}$ und $0 \leq r \leq n \leq n-1$ existieren, sodass $a = nq + r$. Damit ist $[a] = [r]$, also

$$\mathbb{Z} = \bigcup_{r=0}^{n-1} [r].$$

In ähnlicher Weise zeigt man, dass für alle $0 \leq r_1, r_2 \leq n-1$ mit $r_1 \neq r_2$ gilt $[r_1] \neq [r_2]$ (Übung!). Damit bilden die Klassen $[0], [1], [2], \ldots, [n-1]$ eine Partition von $\mathbb{Z}$ bezüglich der Relation $\equiv \pmod{n}$.

2 Gruppen und Symmetrie

Definition 2.1. Ein Paar $(G, \cdot)$, bestehend aus einer Menge G zusammen mit einer Verknüpfung

$$\cdot \colon G \times G \to G, \quad (a, b) \mapsto a \cdot b,$$

heißt eine *Gruppe* mit der *Gruppenoperation* $\cdot$, wenn die folgenden Axiome erfüllt sind:

(G1) (*Assoziativgesetz*) Für alle $a, b, c \in G$ gilt:

$$(a \cdot b) \cdot c = a \cdot (b \cdot c).$$

(G2) (Existenz eines *neutralen Elements*) Es existiert ein $e \in G$, sodass für alle $a \in G$ gilt:

$$a \cdot e = a.$$

Das Element e heißt ein *neutrales Element* oder ein *Neutral*.

(G3) (Existenz von *Inversen*) Für jedes $a \in G$ gibt es ein $a' \in G$, sodass:

$$a \cdot a' = e.$$

Angenommen, es gilt darüber hinaus noch:

(G4) (*Kommutativgesetz*) Für alle $a, b \in G$ gilt:

$$a \cdot b = b \cdot a.$$

Dann ist G eine *kommutative Gruppe* oder eine *abelsche Gruppe*.

Beispiel 2.2.

(1) $(\mathbb{Z}, +)$ ist eine abelsche Gruppe, mit dem Neutral 0, und die Inverse von m ist $-m$ für jedes $m \in \mathbb{Z}$.

(2) $(\mathbb{Q} \setminus \{0\}, \cdot)$ ist eine abelsche Gruppe, mit dem Neutral 1, und die Inverse von m ist $\frac{1}{m}$ für jedes $m \in \mathbb{Q} \setminus \{0\}$.

(3) $(\mathbb{N}, +)$ ist keine Gruppe, da es keine Inversen gibt.

(4) $(\mathbb{Z}\setminus\{0\}, \cdot)$ ist keine Gruppe, da es keine Inversen gibt.

Definition 2.3. Sei $n \in \mathbb{N}_{>0}$ und $M = \{1, 2, \ldots, n\}$. Betrachte die Menge

$$S_n = \{\sigma \colon M \to M \mid \sigma \text{ ist eine Bijektion}\}$$

mit der Operation $\circ$ (also die Verknüpfung von Abbildungen). Dann ist $(S_n, \circ)$ eine Gruppe: und zwar, es gilt:

(G1) $\circ$ ist assoziativ;

(G2) die Abbildung $\mathrm{id}_M \colon M \to M,\ m \mapsto m$ ist das Neutral;

(G3) Für jedes $\sigma \in S_n$ ist die Abbildung σ^{-1} die Inverse von σ.

Die Elemente von S_n heißen *Permutationen* von M, und S_n heißt die *Permutationsgruppe* auf einer Menge von n Elementen. Die Elemente $\sigma \in S_n$ können wir auch durch *Wertetabellen* schreiben:

$$\sigma \colon \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

Notation 2.4. Das Neutral id_M wie in der Definition wird oft einfach mit id bezeichnet und heißt die *Identität in* S_n.

Beispiel 2.5. Betrachte die folgenden Elemente in S_4:

$$\sigma \colon \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}, \quad \tau \colon \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}.$$

Dann gilt:

$$\sigma^{-1} \colon \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}, \quad \tau^{-1} \colon \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}.$$

Ferner gilt:

$$\sigma \circ \tau \colon \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}, \quad \tau \circ \sigma \colon \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix},$$

und insbesondere $\sigma \circ \tau \neq \tau \circ \sigma$. Damit ist S_4 nicht kommutativ. Im Allgemeinen ist S_n für jedes $n \geq 3$ keine abelsche Gruppe.

Satz 2.6. *Für jedes $n \in \mathbb{N}$ gilt $|S_n| = n!$.*

Beweis. Man kann dies mithilfe von Induktion beweisen; ein anderer Beweis lautet:

Für $\sigma(1)$ haben wir n Möglichkeiten. Nachdem wir $\sigma(1)$ ausgewählt haben, haben wir für $\sigma(2)$ noch $n-1$ Möglichkeiten. Im Allgemeinen: Nachdem wir die ersten $k-1$ Werte ausgewählt haben, haben wir für $\sigma(k)$ noch $n-k+1$ Möglichkeiten. Damit ist $|S_n| = n \cdot (n-1) \cdot \ldots \cdot 1 = n!$. □

Bemerkung 2.7. Sei M eine Menge. Die Menge $\mathrm{Abb}(M, M)$ aller Abbildungen zwischen M und M hat die Mächtigkeit $|M|^{|M|}$.

Satz 2.8. *Sei $(G, \cdot)$ eine Gruppe. Dann gelten die folgenden Aussagen.*

(a) Ein neutrales Element e erfüllt auch $e \cdot a = a$.

(b) Das neutrale Element ist eindeutig bestimmt.

(c) Ein inverses Element $a' \in G$ von $a \in G$ erfüllt auch $a' \cdot a = e$.

(d) Das inverse Element eines Elements $a \in G$ ist eindeutig bestimmt. Wir schreiben a^{-1} statt a'.[2]

(e) Für Elemente $a_1, \ldots, a_n \in G$ ist das Element $a_1 \cdot a_2 \cdot \ldots \cdot a_n \in G$ eindeutig bestimmt, egal wie man die Klammern in diesem Produkt setzt.

Beweis.
(c) Da a' ein inverses Element zu a ist, so gilt $a \cdot a' = e$. Ferner, nach $(G3)$ gibt es ein $a'' \in G$, sodass

$$a' \cdot a'' = e. \tag{1}$$

Es folgt:

$$\begin{aligned} a' \cdot a &\overset{(G2)}{=} (a' \cdot a) \cdot e \overset{(1)}{=} (a' \cdot a) \cdot (a' \cdot a'') \\ &\overset{(G1)}{=} a' \cdot (a \cdot (a' \cdot a'')) \overset{(G1)}{=} a' \cdot ((a \cdot a') \cdot a'') \overset{(G3)}{=} a' \cdot (e \cdot a'') \\ &\overset{(G1)}{=} (a' \cdot e) \cdot a'' \overset{(G2)}{=} a' \cdot a'' \overset{(1)}{=} e. \end{aligned}$$

(a) Sei a' ein inverses Element zu a. Dann:

$$e \cdot a \overset{(G3)}{=} (a \cdot a') \cdot a \overset{(G1)}{=} a \cdot (a' \cdot a) \overset{(c)}{=} a \cdot e \overset{(G2)}{=} a.$$

(b) Sei $\widetilde{e}$ ein weiteres neutrales Element. Dann gilt:

$$e \overset{(G2) \text{ für } \widetilde{e}}{=} e \cdot \widetilde{e} \overset{(a)}{=} \widetilde{e}.$$

(d) Sei a' ein inverses Element zu a, und sei $\widetilde{a}$ ein weiteres inverses Element zu a. Nach (c) gilt

$$\widetilde{a} \cdot \ a = e. \tag{2}$$

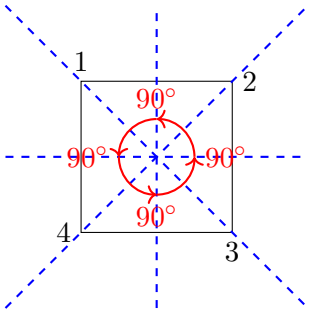
[2] Wenn die Operation auf G mit $+$ bezeichnet wird, dann schreiben wir $-a$ für die Inverse von a.

Dann folgt:

$$\widetilde{a} \overset{(G2)}{=} \widetilde{a} \cdot e \overset{(G3)}{=} \widetilde{a} \cdot (a \cdot a') \overset{(G1)}{=} (\widetilde{a} \cdot a) \cdot a' \overset{(2)}{=} e \cdot a' \overset{(a)}{=} a'.$$

(e) Übung! □

Beispiel 2.9. Mit D_4 bezeichnen wir die folgende Symmetriegruppe des Quadrats:



Die Menge D_4 enthält vier Spiegelungen und vier Drehungen (0°, 90°, 180°, 270°). Das neutrale Element ist die Drehung um 0°.

Sei σ die Drehung um 90°:

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

und sei τ die Spiegelung an der y-Achse:

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

Dann gilt

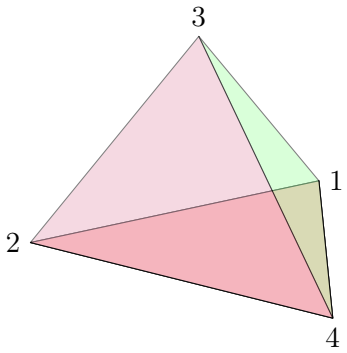
$$\tau \circ \sigma\colon \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} = \text{ Spiegelung an der Diagonale } (1,3)$$

und

$$\sigma \circ \tau\colon \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} = \text{Spiegelung an der Diagonale } (2,4).$$

Insbesondere ist D_4 nicht abelsch. Die Gruppe D_4 ist eine *Untergruppe* von S_4. (Siehe Definition 2.15.)

Beispiel 2.10. Sei T ein Tetraeder:



Übung: Finde alle Elemente der Symmetriegruppe von T geometrisch, und zeige, dass diese Gruppe S_4 ist.

Beispiel 2.11. Gruppen lassen sich auch durch *Verknüpfungstafeln* darstellen. Als Beispiel: Sei $V_4 = \{e, a, b, c\}$ die folgende *Kleinsche Vierergruppe* mit der Verknüpfungstafel:

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Aus der Tafel kann man folgendes sehen:

- $x^2 = e$ für jedes $x \in V_4$;
- e ist das neutrale Element;
- V_4 ist abelsch.

Gruppenhomomorphismen

Definition 2.12. Seien $(G, \cdot_G)$ und $(H, \cdot_H)$ zwei Gruppen. Ein *Gruppenhomomorphismus* von G nach H ist eine Abbildung $\varphi\colon G \to H$, sodass gilt:

$$\forall a, b \in G: \quad \varphi(a \cdot_G b) = \varphi(a) \cdot_H \varphi(b).$$

In anderen Worten: φ ist verträglich mit den Gruppenoperationen $\cdot_G$ und $\cdot_H$ auf G und H.

Zusätzlich ist φ ein:

(a) *Monomorphismus*, wenn φ *injektiv* ist;

(b) *Epimorphismus*, wenn φ *surjektiv* ist;

(c) *Isomorphismus*, wenn φ *bijektiv* ist. In diesem Falle schreiben wir auch $G \cong H$ oder $G \simeq H$. (Ausgesprochen: „G ist isomorph zu H“.)

Satz 2.13. *Seien $(G, \cdot_G)$ und $(H, \cdot_H)$ zwei Gruppen und $\varphi\colon G \to H$ ein Gruppenhomomorphismus. Seien e_G bzw. e_H die neutralen Elemente in G bzw. H. Dann gilt:*

(a) $\varphi(e_G) = e_H$,

(b) $\varphi(a^{-1}) = \varphi(a)^{-1}$ *für jedes* $a \in G$.

Beweis.
(a) Es gilt

$$\varphi(e_G) = \varphi(e_G \cdot e_G) = \varphi(e_G) \cdot \varphi(e_G), \tag{3}$$

und damit

$$\begin{aligned} e_H = \varphi(e_G) \cdot \varphi(e_G)^{-1} &\overset{(3)}{=} \big(\varphi(e_G) \cdot \varphi(e_G)\big) \cdot \varphi(e_G)^{-1} \\ &= \varphi(e_G) \cdot \underbrace{\big(\varphi(e_G) \cdot \varphi(e_G)^{-1}\big)}_{e_H} = \varphi(e_G) \cdot e_H = \varphi(e_G). \end{aligned}$$

(b) Es gilt

$$\varphi(a) \cdot \varphi(a^{-1}) = \varphi(a \cdot a^{-1}) = \varphi(e_G) \overset{(a)}{=} e_H,$$

und damit $\varphi(a^{-1}) = \varphi(a)^{-1}$, wie gewünscht. □

Beispiel 2.14. Sei

$$\exp_a\colon (\mathbb{Z}, +) \to (\mathbb{R}_{>0}, \cdot), \quad n \mapsto a^n,$$

wobei $\mathbb{R}_{>0} = \{x \in \mathbb{R} \mid x > 0\}$ und $a \in \mathbb{R}_{>0} \setminus \{1\}$. Dann ist $\exp_a$ ein Gruppenhomomorphismus, da

$$\exp_a(n_1 + n_2) = a^{n_1+n_2} = a^{n_1} \cdot a^{n_2} = \exp_a(n_1) \cdot \exp_a(n_2).$$

(In der mathematischen Analysis wird dieser Homomorphismus zu einem Homomorphismus $\exp_a\colon (\mathbb{R}, +) \to (\mathbb{R}_{>0}, \cdot)$ fortgesetzt.)

Definition 2.15. Sei $(G, \cdot)$ eine Gruppe und H eine Teilmenge von G. Dann heißt H eine *Untergruppe* von G, wenn:

(1) für alle $a, b \in H$ gilt $a \cdot b \in H$, und

(2) $(H, \cdot)$ bildet eine Gruppe.

Wir schreiben dann auch $H \leq G$.

Beispiel 2.16.

(a) Die Menge aller geraden Zahlen (häufig auch bezeichnet mit $2\mathbb{Z}$) ist eine Untergruppe von $(\mathbb{Z}, +)$.

(b) $(\mathbb{Z}, +)$ ist eine Untergruppe von $(\mathbb{R}, +)$.

(c) Seien H_1 und H_2 zwei Untergruppen einer Gruppe G. Dann ist auch $H_1 \cap H_2$ eine Untergruppe von G. (Übung!)

(d) Sei G eine Gruppe und $A \subseteq G$ eine Teilmenge. Dann ist

$$H = \bigcap_{A \subseteq \widetilde{H} \leq G} \widetilde{H}$$

eine Untergruppe von G (Übung!). Dies ist auch die kleinste Untergruppe, die A enthält. Sie nennen wir auch die *von A erzeugte Untergruppe*, und schreiben

$$H := \langle A \rangle.$$

Wenn $A = \{g_1, \ldots, g_n\}$, dann schreiben wir für diese Gruppe auch $\langle g_1, \ldots, g_n \rangle$.

Beispiel 2.17. Seien $(G, \cdot_G)$ und $(H, \cdot_H)$ zwei Gruppen. Dann ist $G \times H$ eine Gruppe mit der wie folgend definierten Operation $\cdot$ auf $G \times H$:

$$(a, b) \cdot (c, d) := (a \cdot_G c, b \cdot_H d) \quad \text{für alle } a, c \in G, b, d \in H.$$

Das neutrale Element in $G \times H$ ist (e_G, e_H), und es gilt $(a, b)^{-1} = (a^{-1}, b^{-1})$ für alle $(a, b) \in G \times H$.

Satz 2.18. *Sei $(G, \cdot)$ eine Gruppe. Eine nichtleere Teilmenge $H \subseteq G$ ist eine Untergruppe von G genau dann, wenn*

$$\forall a, b \in H : \quad a \cdot b^{-1} \in H. \tag{4}$$

Beweis.
$\Longrightarrow$: Sei H eine Untergruppe von G. Dann ist die Abbildung

$$\theta\colon H \to G, \quad h \mapsto h$$

ein Homomorphismus. Deswegen stimmen, nach Satz 2.13, die neutralen sowie die inversen Elemente in diesen Gruppen überein. Es gilt also:

$$a, b \in H \Longrightarrow a, b^{-1} \in H,$$

und damit ist $a \cdot b^{-1} \in H$ nach der Definition einer Untergruppe.

$\Longleftarrow$: Die Menge H ist nicht leer, und fixiere ein $h \in H$. Damit ist nach (4) (für $a = b = h$):

$$e_G = h \cdot h^{-1} \in H. \tag{5}$$

Für jedes $g \in H$ gilt nach (4) und (5):

$$g^{-1} = e_G \cdot g^{-1} \in H. \tag{6}$$

Seien nun $c, d \in H$. Nach (6) gilt dann $c, d^{-1} \in H$, und dann folgt aus (4):

$$c \cdot (d^{-1})^{-1} \in H.$$

Es gilt also $c \cdot d \in H$, welches zeigt, dass H eine Untergruppe von G ist. □

Satz/Definition 2.19. *Sei $\varphi\colon G \to H$ ein Gruppenhomomorphismus. Der* Kern *von φ ist die Menge*

$$\ker \varphi := \{x \in G \mid \varphi(x) = e_H\} = \varphi^{-1}(e_H),$$

und das Bild von φ ist die Menge $\operatorname{Im} \varphi := \varphi(G) \subseteq H$. *Es gilt:*

(a) der Kern $\ker \varphi$ ist eine Untergruppe von G;

(b) das Bild $\operatorname{Im} \varphi$ ist eine Untergruppe von H.

Beweis.
(a) Sei $b \in \ker \varphi$; äquivalent: $\varphi(b) = e_H$. Dann folgt:

$$\varphi(b^{-1}) \overset{\text{Satz } 2.13}{=} \varphi(b)^{-1} = e_H^{-1} = e_H,$$

und damit

$$b^{-1} \in \ker \varphi. \tag{7}$$

Seien nun $a, b \in \ker \varphi$. Nach (7) gilt dann $a, b^{-1} \in \ker \varphi$, also $\varphi(a) = \varphi(b^{-1}) = e_H$. Es folgt:

$$\varphi(a \cdot b^{-1}) = \varphi(a) \cdot \varphi(b^{-1}) = e_H \cdot e_H = e_H,$$

also $a \cdot b^{-1} \in \ker \varphi$. Nach Satz 2.18 zeigt dies, dass $\ker \varphi$ eine Untergruppe von G ist.

(b) Seien $a, b \in \operatorname{Im} \varphi$. Dann existieren $x, y \in G$ mit $\varphi(x) = a$ und $\varphi(y) = b$, und damit

$$ab^{-1} = \varphi(x)\varphi(y)^{-1} \overset{\text{Satz } 2.13}{=} \varphi(xy^{-1}).$$

In anderen Worten, $ab^{-1} \in \operatorname{Im} \varphi$, welches nach Satz 2.18 zeigt, dass $\operatorname{Im} \varphi$ eine Untergruppe von H ist. □

Definition 2.20. Sei $(G, \cdot)$ eine Gruppe und sei H eine Untergruppe von G. Sei $a \in G$. Die Menge

$$aH := \{a \cdot x \mid x \in H\}$$

heißt die *linke Nebenklasse* von H bezüglich a. Die Menge

$$Ha := \{x \cdot a \mid x \in H\}$$

heißt *rechte Nebenklasse* von H bezüglich a. Die Menge aller linken Nebenklassen von H wird mit

$$G/H$$

bezeichnet; die Menge aller rechten Nebenklassen wird mit

$$H\backslash G$$

bezeichnet. (Ausgesprochen: „G modulo H“.)

Lemma 2.21. *Sei $(G, \cdot)$ eine Gruppe und sei H eine Untergruppe von G. Seien $a, b \in G$. Dann gilt:*

$$aH = bH \iff b^{-1} \cdot a \in H.$$

Beweis.
$\Longrightarrow$: Es gilt:

$$a = ae_G \in aH = bH = \{bx \mid x \in H\}.$$

Damit existiert $x \in H$ mit $a = bx$. Es folgt:

$$b^{-1}a = b^{-1}(bx) = (b^{-1}b)x = x \in H.$$

$\Longleftarrow$: Es reicht zu zeige, dass $aH \subseteq bH$ und $bH \subseteq aH$.
Sei $x := b^{-1}a \in H$. In anderen Worten, $a = bx$. Es folgt:

$$aH = \{ay \mid y \in H\} = \{(bx)y \mid y \in H\} = \{b\underbrace{(xy)}_{\in H} \mid x, y \in H\}$$
$$\subseteq \{bz \mid z \in H\} = bH,$$

also $aH \subseteq bH$. Um die umgekehrte Inklusion zu zeigen, bemerken wir, dass $(b^{-1}a)^{-1} \in H$, da H eine Gruppe ist. Aus $(b^{-1}a)^{-1} = a^{-1}b$ folgt also, dass

$$a^{-1}b \in H.$$

Dann zeigen wir, dass $bH \subseteq aH$, indem wir im obigen Beweis a und b vertauschen. □

Lemma 2.22. *Sei $(G, \cdot)$ eine Gruppe und sei H eine Untergruppe von G. Seien $a, b \in G$. Dann gilt:*

$$aH = bH \Longleftrightarrow aH \cap bH \neq \emptyset.$$

Beweis.
$\Longrightarrow$: Trivial.

$\Longleftarrow$: Sei $y \in aH \cap bH$. Dann existieren $x \in H$ und $z \in H$, sodass

$$y = ax \quad \text{und} \quad y = bz.$$

Es folgt also

$$ax = bz,$$

und damit

$$b^{-1}a = b^{-1}(ax)x^{-1} = b^{-1}(bz)x^{-1} = zx^{-1} \in H.$$

Es folgt aus Satz 2.21, dass $aH = bH$. □

Lemma 2.23. *Sei $(G, \cdot)$ eine endliche Gruppe und sei H eine Untergruppe von G. Dann gilt für alle $a, b \in G$:*

$$|aH| = |bH|.$$

Beweis. Betrachte die Abbildung

$$\varphi\colon aH \to bH, \quad y \mapsto ba^{-1}y.$$

Zuerst zweigen wir, dass die Abbildung φ wohldefiniert ist. Und zwar, da $y \in aH$, so existiert $x \in H$ mit $y = ax$, und damit $ba^{-1}y = bx \in bH$.

Ferner ist φ bijektiv, da die Abbildung

$$\psi\colon bH \to aH, \quad z \mapsto ab^{-1}z$$

die inverse Abbildung zu φ ist. Daraus folgt, dass $|aH| = |bH|$. □

Definition 2.24. Sei $(G, \cdot)$ eine Gruppe und sei H eine Untergruppe von G. Die Mächtigkeit der Menge G/H heißt der *Index* von H und wird mit

$$[G : H]$$

bezeichnet.

Satz 2.25 (Satz von Lagrange)**.** *Sei $(G, \cdot)$ eine endliche Gruppe und sei H eine Untergruppe von G. Dann gilt*

$$|G| = |H| \cdot [G : H].$$

Beweis. Nach Satz 2.22 bilden die Elemente von G/H eine Partition von G, d.h.

$$G = \bigsqcup_{aH \in G/H} aH.$$

Damit gilt

$$|G| = \sum_{aH \in G/H} |aH|.$$

Diese Summe hat $|G/H|$ Summanden und jeder Summand hat $|H|$ Elemente nach Satz 2.23. Es folgt:

$$|G| = |G/H| \cdot |H| = [G : H] \cdot |H|,$$

wie gewünscht. □

Korollar 2.26. *Sei $(G, \cdot)$ eine endliche Gruppe und sei H eine Untergruppe von G. Dann teilt die Zahl $|H|$ die Zahl $|G|$.*

Definition 2.27. Sei $(G, \cdot)$ eine Gruppe. Die Zahl $|G|$ heißt die *Ordnung* von G. Sei zudem $g \in G$ und sei e das neutrale Element von G. Die Zahl

$$\inf\{k \in \mathbb{N}_{>0} \mid g^k = e\}^3$$

heißt die *Ordnung* von g in G, und wird mit $\operatorname{ord}(g)$ bezeichnet. Es gilt also

$$\operatorname{ord}(g) \in \mathbb{N}_{>0} \cup \{\infty\}.$$

Kanonische Projektion

Seien $(G, \cdot)$ und $(H, \cdot)$ Gruppen und sei $\theta\colon G \to H$ ein Gruppenhomomorphismus. Dann ist $\ker\theta$ eine Untergruppe von G nach Satz 2.19, also ist die Menge $G/\ker\theta$ wohldefiniert. Wir werden zeigen, dass diese Menge tatsächlich eine Gruppe ist.

Wenn $g \in G$, dann schreiben wir $[g]$ für das Element $g \cdot \ker\theta \in G/\ker\theta$.

Zuerst brauchen wir das folgende Lemma.

Lemma 2.28. *Seien $(G, \cdot)$ und $(H, \cdot)$ Gruppen und sei $\theta\colon G \to H$ ein Gruppenhomomorphismus. Für jedes $g \in G$ gilt*

$$g \cdot \ker\theta = \ker\theta \cdot g.$$

Beweis. Betrachte die Menge

$$M := g \cdot \ker\theta \cdot g^{-1} := \{gcg^{-1} \mid c \in \ker\theta\}.$$

Es reicht zu zeigen (Übung!), dass $M = \ker\theta$.

$\subseteq$: Sei $z \in M$. Dann gibt es ein $c \in \ker\theta$ mit $z = gcg^{-1}$, und es gilt:

$$\theta(z) = \theta(gcg^{-1}) = \theta(g)\underbrace{\theta(c)}_{=e_H}\theta(g^{-1}) = \theta(g)\theta(g^{-1}) = \theta(g)\theta(g)^{-1} = e_H,$$

damit $z \in \ker\theta$. Es gilt also $M \subseteq \ker\theta$.

$\supseteq$: Sei $c \in \ker\theta$. Setze $z := g^{-1}cg$, und bemerke, dass $z \in \ker\theta$ (wie im ersten Teil des Beweises). Aber dann $c = gzg^{-1} \in M$, welches zeigt, dass $\ker\theta \subseteq M$. □

[3] Hier ist $g^k = \underbrace{g \cdot \ldots \cdot g}_{k \text{ Mal}}$

Wir definieren nun auf $G/\ker\theta$ eine Gruppenoperation. Und zwar, seien $[x], [y] \in G/\ker\theta$, und setze

$$\underbrace{[x] \cdot [y]}_{\text{auf } G/\ker\theta} := \underbrace{[x \cdot y]}_{\text{auf } G}.$$

Diese Verknüpfung ist wohldefiniert, d.h. sie ist unabhängig von der Wahl der Elemente x und y in G. Und zwar, seien $x, x', y, y' \in G$ mit $[x] = [x']$ und $[y] = [y']$. Dann müssen wir zeigen, dass $[x] \cdot [y] = [x'] \cdot [y']$, d.h., dass

$$[xy] = [x'y'].$$

Wir zeigen dies nun. Aus $[x] = [x']$ und $[y] = [y']$ folgt, dass es $a, b \in \ker\theta$ gibt mit $x' = xa$ und $y' = yb$ (dies folgt aus Lemma 2.21). Damit gilt

$$x'y' = (xa)(yb) = x(ay)b. \tag{8}$$

Da $ay \in \ker\theta \cdot y$, und da $y \cdot \ker\theta = \ker\theta \cdot y$ nach Lemma 2.28, so gibt es $a' \in \ker\theta$ mit

$$ay = ya'.$$

Es folgt dann aus (8):

$$(xy)^{-1}x'y' = (xy)^{-1}x(ay)b = (xy)^{-1}x(ya')b = (xy)^{-1}xya'b = a'b \in \ker\theta.$$

Nach Lemma 2.21 zeigt dies, dass $[xy] = [x'y']$, wie gewünscht.

Wir haben also gezeigt, dass $G/\ker\theta$ mit der oben definierten Operation eine Gruppe ist. Es gibt den *kanonischen* oder *natürlichen* Gruppenhomomorphismus

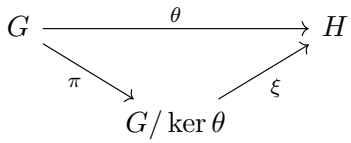
$$\pi\colon G \to G/\ker\theta, \quad g \mapsto [g].$$

Diese Abbildung π heißt auch die *Projektion* von G auf $G/\ker\theta$.

Satz 2.29 (Homomorphiesatz für Gruppen)**.** *Sei $\theta\colon G \to H$ ein Gruppenhomomorphismus. Dann ist $G/\ker\theta$ eine Gruppe mit der kanonischen Projektion $\pi\colon G \to G/\ker\theta$. Es gibt einen wohl-definierten Gruppenhomomorphismus*

$$\xi\colon G/\ker\theta \to H, \quad [g] \mapsto \theta(g),$$

und das Diagramm



kommutiert, d.h. $\theta = \xi \circ \pi$*. Die Abbildung* ξ *induziert den Isomorphismus*

$$\rho\colon G/\ker\theta \to \operatorname{Im}\theta, \quad [g] \mapsto \xi([g]) = \theta(g).$$

Beweis. Wir haben bereits gezeigt, dass $G/\ker\theta$ eine Gruppe ist.

Wir zeigen als Nächstes, dass die Abbildung ξ wohldefiniert ist: in anderen Worten, wenn $[g] = [g']$ für $g, g' \in G$, dann $\xi([g]) = \xi([g'])$, oder äquivalent: $\theta(g) = \theta(g')$. Und zwar, nach Lemma 2.21 gilt $g^{-1}g' \in \ker\theta$, oder äquivalent,

$$e_H = \theta(g^{-1}g') = \theta(g)^{-1}\theta(g').$$

Es gilt also $\theta(g) = \theta(g')$, wie gewünscht.

Per Definition von ξ folgt $\theta = \xi \circ \pi$.

Zuletzt müssen wir zeigen, dass ρ ein Isomorphismus ist. Injektivität: Angenommen, $\rho([g]) = \rho([g'])$ für $g, g' \in G$. Dann gilt $\theta(g) = \theta(g')$ per Definition von ρ, und damit wie oben:

$$e_H = \theta(g^{-1}g').$$

Dies ist äquivalent zu $g^{-1}g' \in \ker\theta$, und dann $[g] = [g']$ nach Lemma 2.21. Surjektivität: Sei $x \in \operatorname{Im}\theta$. Dann existiert $z \in G$ mit $\theta(z) = x$, und damit

$$x = \theta(z) = (\xi \circ \pi)(z) = \xi(\pi(z)) = \xi([z]).$$

Der Satz ist bewiesen. □

Beispiel 2.30.

(a) Die Menge $\mathbb{Z}/\sim$, wobei $\sim$ die Relation $\equiv \pmod n$ ist, ist eine Gruppe mit der Operation

$$[a] + [b] := [a + b] \quad \text{für alle } a, b \in \mathbb{Z}$$

(Übung!). Diese Gruppe wird mit $\mathbb{Z}_n$ oder mit $\mathbb{Z}/n\mathbb{Z}$ bezeichnet (siehe auch (b) unten). Die Elemente von $\mathbb{Z}_n$ sind die Klassen $[0], [1], \ldots, [n-1]$.

(b) Betrachte die Abbildung

$$\varphi\colon \mathbb{Z} \to \mathbb{Z}_n, \quad a \mapsto [a].$$

Dann ist φ ein Gruppenepimorphismus und

$$\ker\varphi = n\mathbb{Z} := \{nx \mid x \in \mathbb{Z}\}.$$

Nach dem Homomorphiesatz folgt, dass

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n.$$

Wenn wir den Beweis von Satz 2.29 noch einmal lesen, dann sehen wir, dass die (fast) einzige Eigenschaft von $\ker\theta$, die wir benutzt haben, ist

$$g \cdot \ker\theta = \ker\theta \cdot g \quad \text{für alle } g \in G.$$

Dies führt zur folgenden Definition.

Definition 2.31. Sei $(G, \cdot)$ eine Gruppe und H eine Untergruppe von G. Dann ist H ein *Normalteiler* oder eine *normale Untergruppe*, falls für alle $g \in G$ gilt

$$gH = Hg,$$

oder äquivalent

$$gHg^{-1} = H.$$

Man zeigt (Übung!), dass G/H eine Gruppe ist, mit der Operation

$$(g_1H) \cdot (g_2H) := (g_1g_2)H \quad \text{für alle } g_1, g_2 \in G.$$

Diese Gruppe heißt die *Quotientengruppe* von G und H.

Beispiel 2.32.

(a) Der Kern eines beliebigen Gruppenhomomorphismus ist ein Normalteiler.

(b) Jede Untergruppe einer abelschen Gruppe ist normal.

Beispiel 2.33. Sei G eine Gruppe und sei $g \in G$. Welche Gruppe ist $\langle g\rangle$ (bis auf Isomorphie)? Wir unterscheiden zwei Fälle:

(a) $\operatorname{ord}(g) = \infty$.
Betrachte die Abbildung

$$\varphi\colon (\mathbb{Z}, +) \to (\langle g\rangle, \cdot), \quad k \mapsto g^k.$$ [4]

Die Abbildung ist ein Gruppenhomomorphismus (Übung!), und sie ist offensichtlich surjektiv. Außerdem ist sie injektiv: für $k \neq \ell$ gilt $g^k \neq g^\ell$. Und zwar, ansonsten wäre

$$g^{k-\ell} = g^{-\ell}g^k = g^{-\ell}g^\ell = e_G,$$

und damit $k = \ell$, da $\operatorname{ord}(g) = \infty$. Die Abbildung φ ist daher ein Isomorphismus.

[4] Hier bedeutet $g^0 := e_G$ und $g^{-k} := (g^k)^{-1} = \underbrace{g^{-1} \cdot \ldots \cdot g^{-1}}_{k \text{ mal}}$.

(b) $n := \operatorname{ord}(g) \in \mathbb{N}_{>0}$.
Betrachte wieder die Abbildung

$$\varphi\colon (\mathbb{Z}, +) \to (\langle g\rangle, \cdot), \quad k \mapsto g^k.$$

Dann ähnlich wie oben kann man zeigen, dass $\ker\varphi = n\mathbb{Z}$ (Übung!). Es folgt nach dem Homomorphiesatz, dass

$$\langle g\rangle \cong \mathbb{Z}/n\mathbb{Z}.$$

Lemma 2.34. *Sei G eine endliche Gruppe und sei $g \in G$. Dann gilt*

$$\operatorname{ord}(g) \mid |G|.$$

Beweis. Sei $n := \operatorname{ord}(g)$. Nach Beispiel 2.32 gilt

$$|\langle g\rangle| = |\mathbb{Z}/n\mathbb{Z}| = n,$$

und nach dem Satz von Lagrange haben wir $|\langle g\rangle| \mid |G|$. Das Lemma folgt. □

Permutationsgruppen

Definition 2.35. Sei $n \in \mathbb{N}_{>0}$ und seien $i_1, i_2, \ldots, i_k \in \{1, \ldots, n\}$ paarweise verschieden. Dann bezeichnet

$$\tau := \begin{pmatrix} i_1 & i_2 & \cdots & i_k \end{pmatrix}$$

die Permutation $\tau \in S_n$ gegeben durch

$$\tau(m) = \begin{cases} i_{j+1}, & \text{wenn } m = i_j \text{ für ein } 1 \le j \le k-1, \\ i_1, & \text{wenn } m = i_k, \\ m, & \text{sonst.} \end{cases}$$

Dann ist τ ein *k-Zyklus* oder *Zyklus der Länge k*.

Beispiel 2.36.

(a) $S_5 \ni \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \end{pmatrix}$.

(b) $S_5 \ni \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 3 & 2 \end{pmatrix}$.

(c) $S_5 \ni \rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \end{pmatrix} \circ \begin{pmatrix} 4 & 5 \end{pmatrix} = \begin{pmatrix} 4 & 5 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \end{pmatrix}$
$\Rightarrow \rho$ ist *kein* Zyklus.

Im Allgemeinen gilt: Für disjunkte Teilmengen $\{i_1, \ldots, i_k\}$ und $\{j_1, \ldots, j_l\}$ von $\{1, \ldots, n\}$ gilt

$$\begin{pmatrix} i_1 & \cdots & i_k \end{pmatrix} \circ \begin{pmatrix} j_1 & \cdots & j_l \end{pmatrix} = \begin{pmatrix} j_1 & \cdots & j_l \end{pmatrix} \circ \begin{pmatrix} i_1 & \cdots & i_k \end{pmatrix},$$

d.h. zwei disjunkte Zyklen kommutieren. (Übung!)

Definition 2.37. Eine *Transposition* in S_n ist ein 2-Zyklus. In anderen Worten, $\tau \in S_n$ ist eine Transposition genau dann, wenn es zwei verschiedene $i, j \in \{1, \ldots, n\}$ gibt, sodass

$$\tau(i) = j, \quad \tau(j) = i \quad \text{und} \quad \tau(k) = k \text{ für } k \neq i, j.$$

Lemma 2.38. *Ist $n \geq 2$, so ist jede Permutation in S_n das Produkt von Transpositionen. In anderen Worten, für jedes $\sigma \in S_n$ existieren Transpositionen $\tau_1, \ldots \tau_k \in S_n$, sodass*

$$\sigma = \tau_1 \circ \cdots \circ \tau_k.$$

Beweis. Sei $\sigma \in S_n$. Angenommen, $\sigma = \mathrm{id}$. Sei τ eine beliebige Transposition. Dann gilt $\sigma = \tau \circ \tau$. Wir dürfen also annehmen, dass $\sigma \neq \mathrm{id}$.

Dann gibt es $i_1 \in \{1, \ldots, n\}$ mit der Eigenschaft, dass

$$\sigma(i) = i \text{ für alle } i < i_1 \quad \text{und} \quad \sigma(i_1) \neq i_1.$$

Insbesondere gilt $\sigma(i_1) > i_1$. Definiere die Transposition

$$\tau_1 := \begin{pmatrix} i_1 & \sigma(i_1) \end{pmatrix} \in S_n,$$

und bezeichne

$$\sigma_1 := \tau_1 \circ \sigma.$$

Dann gilt für jedes $i < i_1$:

$$\sigma_1(i) = (\tau_1 \circ \sigma)(i) = \tau_1(\sigma(i)) = \tau_1(i) = i,$$

und es gilt

$$\sigma_1(i_1) = (\tau_1 \circ \sigma)(i_1) = \tau_1(\sigma(i_1)) = i_1.$$

Damit fixiert die Permutation $\sigma_1 \in S_n$ mindestens die Werte $1, 2, \ldots, i_1$.

Angenommen, $\sigma_1 = \mathrm{id}$. Dann gilt

$$\tau_1^{-1} = \tau_1^{-1} \circ \mathrm{id} = \tau_1^{-1} \circ \sigma_1 = \tau_1^{-1} \circ \tau_1 \circ \sigma = \sigma.$$

Da $\tau_1^{-1} = \tau_1$ eine Transposition ist, so folgt, dass dann σ auch eine Transposition ist.

Wir dürfen also annehmen, dass $\sigma_1 \neq \mathrm{id}$. Nach der Diskussion oben gibt es $i_2 > i_1$, sodass

$$\sigma_1(i) = i \text{ für alle } i < i_2 \quad \text{und} \quad \sigma_1(i_2) \neq i_2.$$

Insbesondere gilt $\sigma_1(i_2) > i_2$. Definiere die Transposition

$$\tau_2 := \begin{pmatrix} i_2 & \sigma_1(i_2) \end{pmatrix} \in S_n,$$

und bezeichne

$$\sigma_2 := \tau_2 \circ \sigma_1.$$

Wie oben zeigt man, dass $\sigma_2(i) = i$ für alle $i \leq i_2$.

Angenommen, $\sigma_2 = \mathrm{id}$. Da $\sigma_2 = \tau_2 \circ \sigma_1 = \tau_2 \circ \tau_1 \circ \sigma$, so zeigt man ähnlich wie oben, dass dann

$$\sigma = (\tau_2 \circ \tau_1)^{-1} = \tau_1^{-1} \circ \tau_2^{-1} = \tau_1 \circ \tau_2.$$

Wir dürfen also annehmen, dass $\sigma_2 \neq \mathrm{id}$. Wir setzen diesen Prozess fort. Der Prozess muss aufhören, da $i_1 < i_2 < \cdots \leq n$. □

Signatur

Definition 2.39. Sei $\sigma \in S_n$. Die *Signatur* oder das *Signum* von σ ist definiert durch die Formel

$$\mathrm{sign}(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i}.$$

Satz 2.40. *Sei $n \in \mathbb{N}_{>0}$. Dann gilt* $\mathrm{sign}(\sigma) \in \{-1, 1\}$ *für jede Permutation $\sigma \in S_n$. Ferner ist die Abbildung*

$$\mathrm{sign} \colon (S_n, \circ) \to (\{-1, 1\}, \cdot)$$

ein Gruppenhomomorphismus. In anderen Worten, für alle $\sigma, \tau \in S_n$ gilt

$$\mathrm{sign}(\sigma \circ \tau) = \mathrm{sign}(\sigma) \cdot \mathrm{sign}(\tau).$$

Beweis. Es gilt

$$\operatorname{sign}(\sigma) = \prod_{1\le i<j\le n} \frac{\sigma(j)-\sigma(i)}{j-i} = \frac{\prod\limits_{1\le i<j\le n}(\sigma(j)-\sigma(i))}{\prod\limits_{1\le i<j\le n}(j-i)}.$$

Da σ eine Permutation ist, kommen im Nenner und im Zähler die gleichen Zahlen vor, nur eventuell mit anderem Vorzeichen. Damit ist $\operatorname{sign}(\sigma) \in \{-1, 1\}$.

Nun beweisen wir die zweite Aussage. Für alle $\sigma, \tau \in S_n$ gilt

$$\begin{aligned}
\operatorname{sign}(\sigma\circ\tau) &= \prod_{1\le i<j\le n} \frac{\sigma(\tau(j))-\sigma(\tau(i))}{j-i} \\
&= \frac{\prod\limits_{1\le i<j\le n}(\sigma(\tau(j))-\sigma(\tau(i)))}{\prod\limits_{1\le i<j\le n}(j-i)} \cdot \underbrace{\frac{\prod\limits_{1\le i<j\le n}(\tau(j)-\tau(i))}{\prod\limits_{1\le i<j\le n}(\tau(j)-\tau(i))}}_{=1} \\
&= \underbrace{\frac{\prod\limits_{1\le i<j\le n}(\sigma(\tau(j))-\sigma(\tau(i)))}{\prod\limits_{1\le i<j\le n}(\tau(j)-\tau(i))}}_{=:C} \cdot \underbrace{\frac{\prod\limits_{1\le i<j\le n}(\tau(j)-\tau(i))}{\prod\limits_{1\le i<j\le n}(j-1)}}_{=:D}.
\end{aligned}$$

Per Definition ist $D = \operatorname{sign}(\tau)$. Es bleibt zu zeigen, dass $C = \operatorname{sign}(\sigma)$.

Und zwar, es gilt

$$\begin{aligned}
C &= \frac{\prod\limits_{1\le i<j\le n}(\sigma(\tau(j))-\sigma(\tau(i)))}{\prod\limits_{1\le i<j\le n}(\tau(j)-\tau(i))} \\
&= \prod_{\substack{1\le i<j\le n\\ \tau(i)<\tau(j)}} \frac{\sigma(\tau(j))-\sigma(\tau(i))}{\tau(j)-\tau(i)} \cdot \prod_{\substack{1\le i<j\le n\\ \tau(j)<\tau(i)}} \frac{\sigma(\tau(j))-\sigma(\tau(i))}{\tau(j)-\tau(i)} \\
&= \prod_{\substack{1\le i<j\le n\\ \tau(i)<\tau(j)}} \frac{\sigma(\tau(j))-\sigma(\tau(i))}{\tau(j)-\tau(i)} \cdot \prod_{\substack{1\le j<i\le n\\ \tau(i)<\tau(j)}} \frac{\sigma(\tau(j))-\sigma(\tau(i))}{\tau(j)-\tau(i)}.
\end{aligned}$$

Da $\tau\colon \{1,\dots,n\} \to \{1,\dots,n\}$ eine Bijektion ist, so ist es einfach zu sehen, dass das letzte Produkt gleich

$$\prod_{1\le k<\ell\le n} \frac{\sigma(\ell)-\sigma(k)}{\ell-k},$$

und das ist genau die Signatur von σ, welches es zu beweisen gab. $\square$

Bemerkung 2.41. In dieser Bemerkung zeigen wir, wie man die Signatur effektiv berechnen kann.

Sei $\sigma \in S_n$ eine Permutation. Ein Paar $(i,j) \in \{1,\dots,n\} \times \{1,\dots,n\}$ heißt ein *Fehlstand* von σ, falls

$$i < j \qquad \text{und} \qquad \sigma(i) > \sigma(j).$$

Sei k die Anzahl der Fehlstände von σ. Dann behaupten wir, dass

$$\operatorname{sign}(\sigma) = (-1)^k. \tag{9}$$

In anderen Worten:

$$\operatorname{sign}(\sigma) = \begin{cases} 1, & \text{falls } \sigma \text{ eine gerade Anzahl der Fehlstände hat,} \\ -1, & \text{falls } \sigma \text{ eine ungerade Anzahl der Fehlstände hat.} \end{cases}$$

Um (9) zu zeigen, berechnen wir:

$$\prod_{1\le i<j\le n} (\sigma(j)-\sigma(i)) = \underbrace{\prod_{\substack{1\le i<j\le n \\ \sigma(j)>\sigma(i)}} (\sigma(j)-\sigma(i))}_{=:A} \cdot \underbrace{\prod_{\substack{1\le i<j\le n \\ \sigma(j)<\sigma(i)}} (\sigma(j)-\sigma(i))}_{=:B},$$

und bemerken, dass

$$A = \prod_{1\le i<j\le n} \underbrace{(\sigma(j)-\sigma(i))}_{>0} = \prod_{1\le i<j\le n} |\sigma(j)-\sigma(i)|$$

und

$$\begin{aligned} B = \prod_{1\le i<j\le n} \underbrace{(\sigma(j)-\sigma(i))}_{<0} &= \prod_{1\le i<j\le n} (-1)\cdot|\sigma(j)-\sigma(i)| \\ &= (-1)^k \cdot \prod_{1\le i<j\le n} |\sigma(j)-\sigma(i)|. \end{aligned}$$

Damit gilt:

$$\begin{aligned} \prod_{1\le i<j\le n} (\sigma(j)-\sigma(i)) = A\cdot B &= (-1)^k \cdot \prod_{1\le i<j\le n} |\sigma(j)-\sigma(i)| \\ &= (-1)^k \cdot \prod_{1\le i<j\le n} (j-i), \end{aligned}$$

wobei die letzte Gleichung folgt, da σ eine Permutation ist. Deswegen:

$$\operatorname{sign}(\sigma) = \frac{\prod\limits_{1\le i<j\le n} (\sigma(j)-\sigma(i))}{\prod\limits_{1\le i<j\le n} (j-i)} = (-1)^k,$$

wie gewünscht.

Beispiel 2.42. Die Permutation $S_4 \ni \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$ hat 4 Fehlstände, und damit ist $\operatorname{sign}(\sigma) = 1$. (Die Fehlstände sind $(1,3), (1,4), (2,3), (2,4)$.)

Korollar 2.43. *Sei $n \ge 2$.*

(a) Für jedes $\sigma \in S_n$ gilt $\operatorname{sign}(\sigma^{-1}) = \operatorname{sign}(\sigma)$.

(b) Für jede Transposition $\tau \in S_n$ gilt $\operatorname{sign}(\tau) = -1$.

(c) Sei $\sigma := \tau_1 \circ \cdots \circ \tau_k \in S_n$ das Produkt von k Transpositionen $\tau_1, \ldots \tau_k \in S_n$. Dann gilt $\operatorname{sign}(\sigma) = (-1)^k$.

Beweis.
Der Teil (c) folgt aus (b) nach Lemma 2.38 und Satz 2.40.

(a) Nach Satz 2.40 gilt

$$1 = \operatorname{sign}(\mathrm{id}) = \operatorname{sign}(\sigma \circ \sigma^{-1}) = \operatorname{sign}(\sigma)\operatorname{sign}(\sigma^{-1}),$$

und damit $\operatorname{sign}(\sigma)^{-1} = \operatorname{sign}(\sigma)$, da beide zur Menge $\{\pm 1\}$ gehören.

(b) Setze $\tau_0 := \begin{pmatrix} 1 & 2 \end{pmatrix}$. Dann hat τ_0 nur einen Fehlstand, und damit ist $\operatorname{sign}(\tau_0) = -1$.

Sei $\tau = \begin{pmatrix} k & l \end{pmatrix} \in S_n$ nun eine beliebige Transposition, wobei $k, \ell \in \{1, \ldots, n\}$ mit $k < \ell$. Sei $\sigma \in S_n$ eine beliebige Permutation mit $\sigma(1) = k$ and $\sigma(2) = \ell$ und setze

$$\tau' := \sigma \circ \tau_0 \circ \sigma^{-1}.$$

Wir behaupten, dass

$$\tau = \tau'. \tag{10}$$

Angenommen, (10) ist bewiesen. Dann gilt nach Satz 2.40 und nach (a):

$$\begin{aligned} \operatorname{sign}(\tau) &= \operatorname{sign}(\sigma \circ \tau_0 \circ \sigma^{-1}) = \operatorname{sign}(\sigma)\operatorname{sign}(\tau_0)\operatorname{sign}(\sigma^{-1}) \\ &= \operatorname{sign}(\sigma)\operatorname{sign}(\sigma^{-1})\operatorname{sign}(\tau_0) = 1 \cdot \operatorname{sign}(\tau_0) = -1, \end{aligned}$$

wie gewünscht.

Es bleibt also zu zeigen (10). Zuerst haben wir:

$$\tau'(k) = \sigma(\tau_0(\sigma^{-1}(k))) = \sigma(\tau_0(1)) = \sigma(2) = \ell = \tau(k),$$
$$\tau'(\ell) = \sigma(\tau_0(\sigma^{-1}(\ell))) = \sigma(\tau_0(2)) = \sigma(1) = k = \tau(\ell).$$

Sei nun $m \in \{1, \dots, n\} \setminus \{k, \ell\}$. Dann ist $\sigma^{-1}(m) \notin \{1, 2\}$, denn ansonsten wäre $m = \sigma(1)$ oder $m = \sigma(2)$, was ein Widerspruch wäre. Es gilt also

$$\tau'(m) = \sigma(\tau_0(\sigma^{-1}(m))) = \sigma(\sigma^{-1}(m)) = m = \tau(m),$$

und dies zeigt (10). Das Korollar ist bewiesen. □

Definition 2.44. Der Kern $A_n := \ker(\text{sign})$ der Abbildung $\text{sign}\colon S_n \to \{\pm 1\}$ heißt *alternierende Gruppe vom Grad n*. In anderen Worten,

$$A_n := \{\sigma \in S_n \mid \text{sign}(\sigma) = 1\}.$$

Lemma 2.45. *Sei $\tau \in S_n$ eine beliebige Transposition. Dann gilt:*

$$S_n = A_n \sqcup \tau A_n.$$

Beweis. Die Vereinigung $A_n \cup \tau A_n$ ist disjunkt, da alle Permutationen aus A_n die Signatur 1 und alle Permutationen aus τA_n die Signatur -1 haben, nach Satz 2.40 und Korollar 2.43.

Sei nun $\sigma \in S_n$. Dann $\text{sign}(\sigma) = \pm 1$. Wenn $\text{sign}(\sigma) = 1$, dann $\sigma \in A_n$ per Definition. Wenn $\text{sign}(\sigma) = -1$, dann $\sigma = \tau \circ (\tau^{-1}\sigma)$, und es gilt $\tau^{-1}\sigma \in A_n$ nach Satz 2.40 und Korollar 2.43. □

Korollar 2.46. *Sei $n \geq 2$. Dann gilt $|A_n| = n!/2$.*

Beweis. Nach Lemma 2.23 gilt $|A_n| = |\tau A_n|$. Lemma 2.45 ergibt:

$$|S_n| = |A_n| + |\tau A_n| = 2|A_n|,$$

und das Korollar folgt, da $|S_n| = n!$. □

3 Ringe und Körper

Definition 3.1. Ein *Körper* ist ein Tripel $(K, +, \cdot)$ aus einer Menge K und zwei Verknüpfungen

$$+\colon K \times K \to K, \quad (a, b) \mapsto a + b,$$
$$\cdot\colon K \times K \to K, \quad (a, b) \mapsto a \cdot b,$$

sodass die folgenden Axiome erfüllt sind:

(K1) $(K, +)$ ist eine abelsche Gruppe mit neutralem Element 0, d.h.:

- (K1.1) $(a + b) + c = a + (b + c)$ für alle $a, b, c \in K$,
- (K1.2) $a + b = b + a$ für alle $a, b \in K$,
- (K1.3) $0 + a = a + 0 = a$ für alle $a \in K$,
- (K1.4) für jedes $a \in K$ gibt es $-a \in K$, sodass $a + (-a) = (-a) + a = 0$.

(K2) $(K \setminus \{0\}, \cdot)$ ist eine abelsche Gruppe mit neutralem Element 1, und es gilt ferner:

- (K2.1) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ für alle $a, b, c \in K$,
- (K2.2) $a \cdot b = b \cdot a$ für alle $a, b \in K$,
- (K2.3) $1 \cdot a = a \cdot 1 = a$ für alle $a \in K$,
- (K2.4) für jedes $a \in K \setminus \{0\}$ gibt es $a^{-1} \in K \setminus \{0\}$, sodass $a \cdot a^{-1} = a^{-1} \cdot a = 1$.

(K3) Es gelten die folgenden *Distributivgesetze*: für alle $a, b, c \in K$ gilt

$$(a + b) \cdot c = a \cdot c + b \cdot c \quad \text{und} \quad a \cdot (b + c) = a \cdot b + a \cdot c.$$

Beispiel 3.2. Bekannte Körper sind $(\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot)$ und $(\mathbb{C}, +, \cdot)$. Die Struktur $(\mathbb{Z}, +, \cdot)$ ist kein Körper, da es keine multiplikativen Inversen gibt.

Definition 3.3. Ein *Ring* ist ein Tripel $(R, +, \cdot)$ aus einer Menge R und zwei Verknüpfungen $+$ und $\cdot$, für welches die Axiome

$$(K1.1) - (K1.4), \qquad (K2.1) \qquad \text{und} \qquad (K3)$$

erfüllt sind.
Falls zusätzlich das Axiom $(K2.2)$ erfüllt ist, so ist R ein *kommutativer* Ring. Falls zusätzlich das Axiom $(K2.3)$ erfüllt ist, so ist R ein kommutativer Ring *mit Eins*.

Beispiel 3.4.

(a) $(\mathbb{Z}, +, \cdot)$ ist ein kommutativer Ring mit 1.

(b) Jeder Körper ist ein kommutativer Ring mit 1.

(c) $(2\mathbb{Z}, +, \cdot)$ ist ein kommutativer Ring ohne 1.

Lemma 3.5. *Jeder Körper hat mindestens zwei Elemente:* 0 *und* 1. *Der kleinste Körper hat zwei Elemente: das ist* $(\mathbb{F}_2, +\cdot)$ *mit* $\mathbb{F}_2 := \{0, 1\}$ *und den Verknüpfungstafeln:*

$+$	0	1
0	0	1
1	1	0

und

$\cdot$	0	1
0	0	0
1	0	1

Insbesondere gilt: Die Gruppe $(\mathbb{F}_2, +)$ *ist* $(\mathbb{Z}_2, +)$. *Die zwei Operationen oben sind* $+$ *und* $\cdot$ *modulo* 2.

Beispiel 3.6. Für jede positive ganze Zahl n ist $(\mathbb{Z}_n, +, \cdot)$ ein Ring (Übung!), wobei

$$[a] + [b] := [a + b] \qquad \text{und} \qquad [a] \cdot [b] := [ab].$$

Ab jetzt schreiben wir in einem Körper:

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

Lemma 3.7. *Sei* $(K, +, \cdot)$ *ein Körper. Dann gilt:*

(1) 0 *und* 1 *sind eindeutig bestimmt,*

(2) das Negative $-a$ *zu* a *und das Inverse* a^{-1} *zu* a *sind eindeutig bestimmt,*

(3) (a) $0 \cdot a = 0$ *für alle* $a \in K$,

(b) $(-1)(-1) = 1$,

(c) aus $ab = 0$ *und* $a \neq 0$ *folgt, dass* $b = 0$.

(4) In endlichen Summen und Produkten kommt es nicht auf die Reihenfolge an. Das heißt: Seien $a_1, \ldots, a_n \in K$ *und sei* $\sigma \in S_n$. *Dann gilt*

$$\sum_{i=1}^{n} a_i = \sum_{i=1}^{n} a_{\sigma(i)} \quad \textit{und} \quad \prod_{i=1}^{n} a_i = \prod_{i=1}^{n} a_{\sigma(i)}.$$

Beweis.
(1) und (2) folgen aus der Tatsache, dass $(K,+)$ und $(K,\cdot)$ Gruppen sind.

(4) folgt aus den Assoziativ- und Kommutativgesetzen.

(3)(a) Es gilt

$$0 \cdot a \overset{(K1.3)}{=} (0+0) \cdot a \overset{(K3)}{=} 0 \cdot a + 0 \cdot a,$$

und damit

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

(3)(b) Es gilt

$$1 + (-1) = 0,$$

und damit

$$(1 + (-1)) \cdot (-1) = 0 \cdot (-1).$$

Dann folgt aus (K3) und aus (3)(a):

$$-1 + (-1)(-1) = 0,$$

und damit

$$(-1)(-1) = 1.$$

(3)(c) Aus $ab = 0$ folgt, nach (3)(a):

$$b = \underbrace{a^{-1}a}_{=1} b = a^{-1}(ab) = a^{-1} \cdot 0 = 0,$$

wie gewünscht. □

Definition 3.8. Sei $(K,+,\cdot)$ ein Körper. Ein *Unterkörper* oder *Teilkörper* $(L,+,\cdot)$ von $(K,+,\cdot)$ besteht aus einer Teilmenge $L \subseteq K$, die bezüglich der bestehenden Verknüpfungen $+$ und $\cdot$ zu einem Körper wird.

Analog dazu ist ein *Unterring* oder *Teilring* definiert.

Definition 3.9. Seien $(R_1,+,\cdot)$ und $(R_2,+,\cdot)$[5] zwei Ringe mit Eins. Eine Abbildung $\varphi\colon R_1 \to R_2$ ist ein *Ringhomomorphismus*, falls:

(1) $\varphi(1_{R_1}) = 1_{R_2}$,

(2) $\varphi(a+b) = \varphi(a) + \varphi(b)$ für alle $a, b \in R_1$,

(3) $\varphi(ab) = \varphi(a)\varphi(b)$ für alle $a, b \in R_1$.

[5] Wir bezeichnen die Operationen in R_1 und in R_2 mit denselben Symbolen.

Falls R_1 und R_2 Körper sind, so ist φ ein *Körperhomomorphismus*.

Bemerkung 3.10. Sei $\varphi\colon R_1 \to R_2$ ein Ringhomomorphismus. Dann gilt

$$\varphi(0_{R_1}) = 0_{R_2},$$

denn φ ist ein Gruppenhomomorphismus zwischen $(R_1, +)$ und $(R_2, +)$.

Lemma 3.11. *Sei $(K, +, \cdot)$ ein Körper und L eine nichtleere Teilmenge von K. Dann ist $(L, +, \cdot)$ ein Teilkörper von K genau dann, wenn:*

(a) $0, 1 \in L$,

(b) für alle $a, b \in L$ *gilt* $a + b \in L$ *und* $ab \in L$,

(c) für alle $a \in L$ *gilt* $-a \in L$ *und* $a^{-1} \in L$.

Beweis. Übung! (Ähnlich wie für Gruppen und Untergruppen.) □

Beispiel 3.12.

(1) Die Abbildung
$$\varphi\colon (\mathbb{Z}, +, \cdot) \to (\mathbb{F}_2, +, \cdot),\ n \mapsto [n]$$
ist ein Ringhomomorphismus. (Übung!)

(2) $(\mathbb{Q}, +, \cdot)$ ist ein Teilkörper von $(\mathbb{R}, +, \cdot)$.

(3) $(\mathbb{R}, +, \cdot)$ ist ein Teilkörper von $(\mathbb{C}, +, \cdot)$.

Notation 3.13. Sei R ein Ring mit 1, Seien $n \in \mathbb{Z}$ und $a \in R$. Dann bezeichnen wir

$$n \cdot a := \begin{cases} \underbrace{a + \cdots + a}_{n \text{ Mal}}, & \text{wenn } n > 0, \\ 0, & \text{wenn } n = 0, \\ \underbrace{-a - \cdots - a}_{(-n) \text{ Mal}}, & \text{wenn } n < 0. \end{cases}$$

Beispiel 3.14.

(1) Für $1 \in \mathbb{Z}$ gilt $n \cdot 1 \neq 0$ für alle $n \in \mathbb{Z} \setminus \{0\}$.

(2) Für jedes $n \in \mathbb{N}_{>0}$ gilt im Ring $\mathbb{Z}_n$: $n \cdot [1] = [n] = [0]$.

Definition 3.15. Sei R ein Ring mit 1. Die *Charakteristik* von R, geschrieben $\operatorname{char}(R)$, ist definiert durch

$$\operatorname{char}(R) := \begin{cases} 0, & \text{falls } n \cdot 1 \neq 0 \text{ für alle } n \in \mathbb{Z} \setminus \{0\}, \\ \min\{n \in \mathbb{N}_{>0} \mid n \cdot 1 = 0\}, & \text{sonst.} \end{cases}$$

Lemma 3.16. *Sei K ein Körper. Dann ist* $\operatorname{char}(K)$ *eine Primzahl oder* 0.

Beweis. Sei $n := \operatorname{char}(K)$. Angenommen, $n \neq 0$. Wir müssen zeigen, dass n eine Primzahl ist.

Angenommen, n ist keine Primzahl. Dann gibt es ganze Zahlen $1 < k, \ell < n$ mit $n = k\ell$, und es folgt:

$$\begin{aligned}(k \cdot 1) \cdot (\ell \cdot 1) &= (\underbrace{1 + \cdots + 1}_{k \text{ Mal}})(\underbrace{1 + \cdots + 1}_{\ell \text{ Mal}}) \overset{(K3)}{=} \underbrace{1 \cdot 1 + \cdots + 1 \cdot 1}_{k \cdot \ell \text{ Mal}} \\ &= \underbrace{1 + \cdots + 1}_{n \text{ Mal}} = n \cdot 1 = 0.\end{aligned}$$

Dann folgt aus Lemma 3.7, dass $k \cdot 1 = 0$ oder $\ell \cdot 1 = 0$. Insbesondere ist $n = \operatorname{char}(K) \leq k$ oder $n = \operatorname{char}(K) \leq \ell$, welches ein Widerspruch ist. □

Komplexe Zahlen

Das Problem mit dem Körper $\mathbb{R}$ ist, dass die Gleichung

$$x^2 + 1 = 0$$

keine Lösung in $\mathbb{R}$ hat. Betrachte nun das Tripel $(\mathbb{R}^2, +, \cdot)$, wobei für alle $a, b, c \in \mathbb{R}$ gilt:

$$\begin{aligned}(a, b) + (c, d) &:= (a + c, b + d), \\ (a, b) \cdot (c, d) &:= (ac - bd, ad + bc).\end{aligned}$$

Dann checkt man einfach, dass $(\mathbb{R}^2, +, \cdot)$ ein Körper ist. Diesen Körper bezeichnen wir mit $(\mathbb{C}, +, \cdot)$. Die neutralen Elemente sind $(0, 0)$ (bezüglich der Operation $+$) und $(1, 0)$ (bezüglich der Operation $\cdot$).

Sei nun $(a, b) \neq (0, 0)$. Dann sind die zu (a, b) inversen Elemente:

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

Lemma 3.17.

(a) Die Teilmenge $K := \{(a,0) \mid a \in \mathbb{R}\} \subseteq \mathbb{C}$ *ist ein Teilkörper von* $\mathbb{C}$.

(b) Die Abbildung $\varphi\colon \mathbb{R} \to K, \quad a \mapsto (a,0)$ *ist ein Körperisomorphismus.*

Beweis. Übung! □

Wegen dieses Lemmas identifizieren wir $\mathbb{R}$ mit K, und wir nennen K den *Körper der reellen Zahlen*. Für $(a,0)$ schreiben wir wie üblich einfach a.

Bemerkung 3.18. Definiere

$$i := (0,1) \in \mathbb{C}.$$

Dann gilt $i^2 = (0,1) \cdot (0,1) = (-1,0) = -1$, und damit ist i eine Lösung der Gleichung $x^2 + 1 = 0$ in $\mathbb{C}$. (Die andere Lösung ist $-i$.) Des Weiteren gilt:

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

Definition 3.19. Betrachte eine komplexe Zahl $z = x + iy$, wobei $x, y \in \mathbb{R}$.

(a) Die reelle Zahl x ist der *Realteil* von z, und wir schreiben

$$\mathrm{Re}(z) := x.$$

(b) Die reelle Zahl y ist der *Imaginärteil* von z, und wir schreiben

$$\mathrm{Im}(z) := y.$$

(c) Die komplexe Zahl $\overline{z} := x - iy$ ist die *zu z konjugierte* komplexe Zahl.

(d) Die reelle Zahl $\sqrt{x^2 + y^2}$ ist der *Absolutbetrag* von z, und wir schreiben

$$|z| := \sqrt{x^2 + y^2}.$$

(e) Die komplexe Zahl z heißt *reell*, falls $\mathrm{Im}(z) = 0$. Sie heißt *imaginär*, falls $\mathrm{Re}(z) = 0$.

Proposition 3.20. *Für jede komplexe Zahl* $z \in \mathbb{C}$ *gilt:*

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

(b) $z - \overline{z} = 2\,\mathrm{Im}(z)$,

(c) $z \cdot \overline{z} = |z|^2$.

Beweis. Einfach (Übung!). □

Proposition 3.21. *Für komplexe Zahlen* $z_1, z_2 \in \mathbb{C}$ *gilt:*

(a) $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$,

(b) $\overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2}$,

(c) $\overline{\left(\frac{1}{z_1}\right)} = \frac{1}{\overline{z_1}}$,

(d) $\overline{\overline{z_1}} = z_1$,

(e) $|\overline{z_1}| = |z_1|$.

Beweis. Einfach (Übung!). □

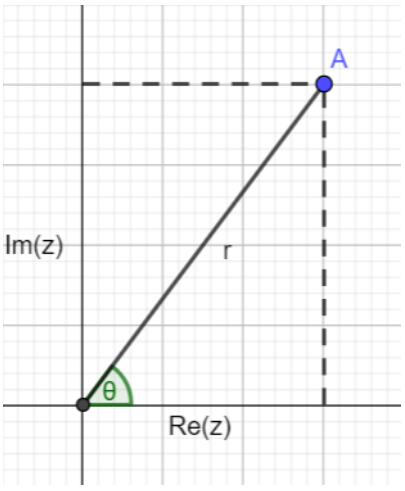
Bemerkung 3.22. Sei $z \neq 0$ eine komplexe Zahl. Dann gilt

$$\frac{1}{z} = \frac{\overline{z}}{z\overline{z}} \overset{3.20(c)}{=} \frac{\overline{z}}{|z|^2},$$

und damit

$$\mathrm{Re}\left(\frac{1}{z}\right) = \frac{1}{|z|^2}\,\mathrm{Re}(\overline{z}) \quad \text{und} \quad \mathrm{Im}\left(\frac{1}{z}\right) = \frac{1}{|z|^2}\,\mathrm{Im}(\overline{z}).$$

Bemerkung 3.23 (Geometrische Darstellung komplexer Zahlen)**.**
Sei $z = a + bi$ eine komplexe Zahl. Dann können wir z in der Zahlenebene $\mathbb{R}^2$ geometrisch darstellen:



Auf dem Bild ist der Punkt $A := (a, b)$ und die Länge r des Segments zwischen 0 und A ist der Betrag $|z|$. Der Winkel θ nennen wir das *Argument von z*. Dann gilt:

$$a = r\cos\theta, \quad b = r\sin\theta, \quad \frac{b}{a} = \tan\theta.$$

Insbesondere gilt

$$z = |z|(\cos\theta + i\sin\theta).$$

Wir schreiben auch

$$z := e^{i\theta} := \cos\theta + i\sin\theta.$$

Lemma 3.24. *Betrachte zwei komplexen Zahlen:*

$$z_1 = r_1(\cos\theta_1 + i\sin\theta_1) \quad \textit{und} \quad z_2 = r_2(\cos\theta_2 + i\sin\theta_2).$$

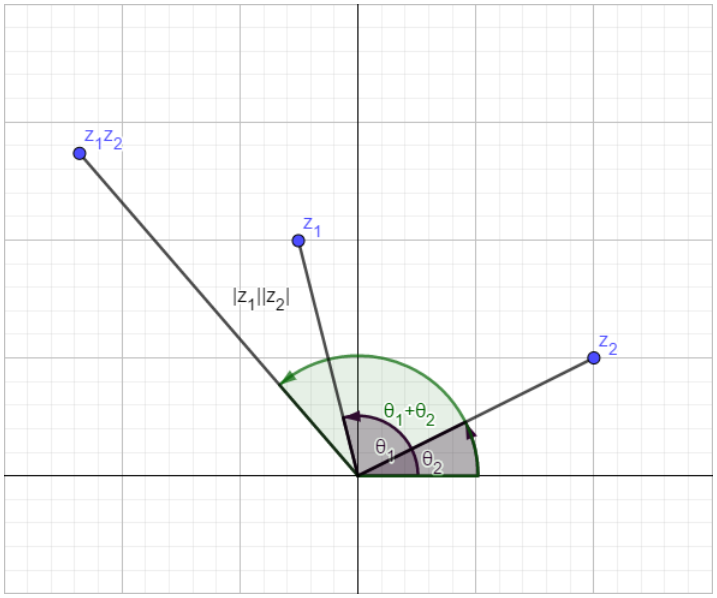
Dann gilt das Gesetz von De Moivre:

$$z_1 z_2 = r_1 r_2\big(\cos(\theta_1 + \theta_2) + i\sin(\theta_1 + \theta_2)\big).$$

Insbesondere gilt

$$z_1^n = r_1^n\big(\cos(n\theta_1) + i\sin(n\theta_1)\big) \quad \textit{für alle } n \in \mathbb{N}_{>0}.$$

In anderen Worten: Bei der Multiplikation komplexer Zahlen multiplizieren sich die Beträge und addieren sich die Argumente.



Beweis. Es gilt:

$$\begin{aligned} z_1 z_2 &= r_1(\cos\theta_1 + i\sin\theta_1) r_2(\cos\theta_2 + i\sin\theta_2) \\ &= r_1 r_2(\cos\theta_1\cos\theta_2 + i\cos\theta_1\sin\theta_2 + i\sin\theta_1\cos\theta_2 - \sin\theta_1\sin\theta_2) \\ &= r_1 r_2\big(\cos(\theta_1+\theta_2) + i\sin(\theta_1+\theta_2)\big), \end{aligned}$$

welches die erste Formel beweist. Die zweite Formel folgt aus dieser per Induktion nach n. □

Polynome

Es gibt zwei mögliche naive Definitionen von Polynomen.

(1) Ein *Polynom* (über einem Körper K) ist eine Formel

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n,$$

wobei $n \in \mathbb{N}$ und a_i sind Elemente aus K. Hier ist x eine *Unbekannte* oder eine *Variable*. Problem: Wie definiert man, was eine Unbekannte ist?

(2) Ein *Polynom* (über einem Körper K) ist eine Abbildung

$$f\colon K \to K, \quad x \mapsto a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n,$$

wobei $n \in \mathbb{N}$ und a_i sind Elemente aus K. Problem: Dies Funktioniert nicht über endlichen Körpern. Betrachte zum Beispiel $K := \mathbb{F}_2$ mit zwei Abbildungen:

$$\begin{aligned} f\colon \mathbb{F}_2 \to \mathbb{F}_2, &\quad x \mapsto x, \\ g\colon \mathbb{F}_2 \to \mathbb{F}_2, &\quad x \mapsto x^2. \end{aligned}$$

Diese zwei Funktionen sind gleich.

Die echte Definition eines Polynoms ist wie folgt.

Definition 3.25. Sei R ein kommutativer Ring mit 1. Bezeichne

$$\begin{aligned} R^{(\mathbb{N})} &:= \{f\colon \mathbb{N} \to \mathbb{R} \mid \text{ alle bis auf endlich viele } f(i) \text{ sind } 0\} \\ &= \{f\colon \mathbb{N} \to \mathbb{R} \mid \exists n \in \mathbb{N} : f(i) = 0 \ \forall i > n\}. \end{aligned}$$

Ein Element $f \in R^{(\mathbb{N})}$ können wir f tabellarisch schreiben als

$$f = (a_0, a_1, a_2, a_3, \dots), \quad \text{wobei } a_i = f(i) \text{ für jedes } i.$$

Auf der Menge $R^{(\mathbb{N})}$ definieren wir zwei Verknüpfungen $+$ und $\cdot$ wie folgt. Seien $f = (a_0, a_1, \dots)$ und $g = (b_0, b_1, \dots)$ zwei Elemente aus $R^{(\mathbb{N})}$. Dann definieren wir

$$f + g := (a_0 + b_0, a_1 + b_1, \dots),$$

und

$$f \cdot g := (c_0, c_1, \dots), \quad \text{wobei } c_k := \sum_{i+j=k} a_i b_j.$$

Man prüft einfach, dass $(R^{(\mathbb{N})}, +, \cdot)$ ein kommutativer Ring mit Eins ist. Diesen Ring nennen wir den *Polynomring in einer Variable über R* oder den *Polynomring in einer Variable mit Koeffizienten in R.*

Die Null in diesem Ring ist das Element $(0, 0, 0, \dots)$. Die Eins in diesem Ring ist das Element $(1, 0, 0, \dots)$. Die *Unbekannte* oder die *Variable* in diesem Ring ist das Element $x := (0, 1, 0, 0, \dots)$. Daraus folgt

$$x^n = (\underbrace{0}_{\text{0-te Stelle}}, \dots, 0, \underbrace{1}_{n\text{-te Stelle}}, 0, \dots).$$

Diesen Ring bezeichnen wir üblicherweise mit

$$R[x].$$

Der Ring R ist isomorph zum Unterring

$$\{(a, 0, 0, \dots) \mid a \in R\} \subseteq R[x].$$

Aus den Definitionen von $+$ und $\cdot$ folgt sofort, dass ein Element

$$f := (a_0, a_1, a_2, \dots)$$

geschrieben werden kann als

$$f = a_0 + a_1 x + a_2 x^2 + \dots.$$

Die Elemente $a_0, a_1, \dots \in R$ nennen wir *Koeffizienten* von f. Aus der Definition von $R[x]$ folgt, dass für nur endlich viele $i \in \mathbb{N}$ gilt $a_i \neq 0$. Wenn $f \neq 0$, dann können wir f also schreiben als

$$f = a_0 + a_1 x + \dots + a_n x^n \quad \text{für ein } n \in \mathbb{N} \text{ mit } a_n \neq 0.$$

Diese Zahl n nennen wir den *Grad von f* und wir schreiben

$$\deg(f) := n.$$

Der Koeffizient a_n heißt der *Leitkoeffizient*. Wenn $f = 0$ ist, dann setzen wir

$$\deg(f) := -\infty.$$

In anderen Worten,

$$\deg(f) = \begin{cases} -\infty, & \text{wenn } f = 0, \\ \max\{k \in \mathbb{N} \mid a_k \neq 0\}, & \text{sonst.} \end{cases}$$

Ein Polynom $f \neq 0$ heißt *normiert* oder *monisch*, falls sein Leitkoeffizient gleich 1 ist.

Bemerkung 3.26. Sei K ein Körper. Für alle $f, g \in K[x]$ gilt

$$\deg(fg) = \deg f + \deg g.$$

(Hier gelten die Regeln $(-\infty) + n = n + (-\infty) = -\infty$.) Dies ist einfach zu zeigen: Wir dürfen annehmen, dass $f \neq 0$ und $g \neq 0$. Wir können dann schreiben

$$f\colon a_0 + a_1 x + \cdots + a_n x^n \text{ mit } a_n \neq 0,$$

und

$$g\colon b_0 + b_1 x + \cdots + b_m x^m \text{ mit } b_m \neq 0.$$

Dann ist $\deg f = n$ und $\deg g = m$, und man checkt einfach, dass der Leitkoeffizient von fg gleich $a_n b_m$ (bemerke, dass $a_n b_m \neq 0$, da $a_n \neq 0$ und $b_m \neq 0$: hier benutzen wir die Voraussetung, dass K ein Körper ist). Es gilt also $\deg(fg) = n + m$.

Insbesondere zeigt dasselbe Argument:

Lemma 3.27. *Sei K ein Körper. Für alle $f, g \in K[x]$ gilt:*

$$fg = 0 \quad \Longrightarrow \quad f = 0 \text{ oder } g = 0.$$

Division mit Rest

In einem Polynomring gilt Division mit Rest, ähnlich wie im Ring $\mathbb{Z}$.

Satz 3.28. *Sei K ein Körper und seien $g, f \in K[x]$ mit $g \neq 0$. Dann gibt es eindeutig bestimmte Polynome $q, r \in K[x]$ mit*

$$f = gq + r, \quad \text{wobei } \deg r < \deg g.$$

Beweis. Zuerst beweisen wir die Eindeutigkeit. Angenommen, es gibt Polynome $q_1, q_2, r_1, r_2 \in K[x]$ mit

$$f = gq_1 + r_1 \quad \text{und} \quad f = gq_2 + r_2, \quad \text{wobei } \deg r_1, \deg r_2 < \deg g.$$

Dann gilt:

$$0 = f - f = (gq_1 + r_1) - (gq_2 + r_2) = g(q_1 - q_2) + (r_1 - r_2),$$

und damit

$$r_2 - r_1 = g(q_1 - q_2).$$

Also gilt:

$$\deg g > \deg(r_2 - r_1) = \deg(g(q_1 - q_2)) = \deg g + \deg(q_1 - q_2).$$

Das ist möglich nur, wenn $\deg(q_1 - q_2) = -\infty$, also $q_1 = q_2$. Dann folgt einfach, dass $r_1 = r_2$.

Nun zeigen wir die Existenz per Induktion nach $\deg f$. Die Aussage ist einfach, wenn $f = 0$; wir nehmen daher an, dass $f \neq 0$. Seien $n := \deg f$ und $m := \deg g$. Dann können wir schreiben

$$f = a_n x^n + \cdots + a_0 \quad \text{und} \quad g = b_m x^m + \cdots + b_0, \text{wobei } a_n, b_m \neq 0.$$

Angenommen zuerst, dass $n < m$. Dann ist $q = 0$ und $r = f$, da $f = g \cdot 0 + f$.

Nun nehmen wir an, dass $n = m$. Setze $q := \frac{a_n}{b_n} \in K$ und $r := f - qg$. Dann checkt man einfach, dass

$$r = \sum_{i=0}^{n-1} (a_i - qb_i) x^i,$$

und daher ist r ein Polynom des Grades $\leq n - 1$.

Zuletzt nehmen wir an, dass $n > m$. Setze $q_1 := \frac{a_n}{b_m} x^{n-m} \in K[x]$ und $r_1 := f - gq_1$. Dann berechnet man einfach, dass

$$r_1 = \sum_{i=0}^{n-1} \left(a_i - \frac{a_n}{b_m} b_{i-m} \right) x^i.$$

Daher ist r_1 ein Polynom des Grades $\leq n - 1 < \deg f$. Damit können wir die Induktion anwenden auf die Polynome r_1 und g: Es gibt $q_2, r_2 \in K[x]$ mit $r_1 = gq_2 + r_2$, wobei $\deg r_2 < \deg g$. Damit gilt:

$$f = gq_1 + r_1 = gq_1 + (gq_2 + r_2) = g(q_1 + q_2) + r_2.$$

Setze nun $q := q_1 + q_2$ und $r := r_2$. Das sind die gewünschten Polynome. $\square$

Beispiel 3.29. Sei $K = \mathbb{R}$ und seien $f, g \in \mathbb{R}[x]$ die Polynome

$$f = 3x^3 + 2x + 1 \qquad \text{und} \qquad g = 4x^2 - 4.$$

Dann gilt:[6]

$$\begin{aligned} &(3x^3 + 2x + 1) : (4x^2 - 4) = \frac{3}{4}x + 0 \\ -&\underline{(3x^2 - 3x)} \\ &\qquad 5x + 1 \end{aligned}$$

Setze $q := \frac{3}{4}x$ und $r := 5x + 1$. Man prüft, dass $f = gq + r$.

[6] $3x^2 - 3x = \frac{3}{4}x \cdot (4x^2 - 4)$