1 Grundlagen

1.1 Mengenlehre

1.1.1 Erste Definitionen und Beispiele

Die Mengenlehre ist einen nicht trivialen Teil der Mathematik. Wir werden Mengen nicht richtig definieren.

Wir werden mit den folgenden vagen (aber für unseren Zwecke ausreichenden) Definition arbeiten.

Definition 1.1.1 Eine **Menge** M ist eine Zusammenfassung von verschiedenen Objekte (die man **Elemente** nennt) zu einem neuen Objekt.

Axiom 1.1.2 (Extensionalitätsaxiom) Zwei Mengen M und N sind genau dann **gleich**, wenn sie die selbe Elementen enthalten.

Notation 1.1.3 Wir werden die folgende Symbole benutzen.

$\{\ \}$	die Mengenklammern:	z.b. $M = \{0; 1; 2\}$.
$\in$	ist Element von:	z.b. $1 \in \{0; 1; 2\}$.
$\notin$	ist nicht Element von:	z.b. $3 \notin \{0; 1; 2\}$.
$\forall$	alle:	z.b. $\forall n \in \mathbb{N}$ es gilt $n \geq 0$.
$\exists$	es gibt:	z.b. $\exists n \in \mathbb{N}$ so dass $n \geq 5$.
$\Rightarrow$	dann:	z.b. $n \geq 1 \Rightarrow n \geq 0$.

Bemerkung 1.1.4 Mit Symbole: $M = N$ genau dann, wenn

$$x \in M \Rightarrow x \in N \text{ und } x \in N \Rightarrow x \in M.$$

Definition 1.1.5 Sei M eine Menge.

1. Eine **Teilemenge** N von einer Menge M ist eine Menge so dass alle elemente in N auch in M enthalten sind. Mit Symbole: $x \in N \Rightarrow x \in M$.

2. Eine **echte** Teilmenge N von einer Menge M ist eine Teilmenge die nicht gleich M ist.

Notation 1.1.6 Hier sind weitere Symbole.

$\subseteq, \subset$	ist Teilmenge von:	z.b. $\{0;1;2\} \subseteq \{0;1;2\}$ oder $\mathbb{N} \subseteq \mathbb{Z}$.
$\subsetneq$	ist eine echte Teilmenge von:	z.b. $\{1;2\} \subsetneq \{0;1;2\}$.

Bemerkung 1.1.7 Es gilt $\{0;1;2\} = \{2;0;1\} = \{0;0;1;2;2;2\}$.

1.1.2 Konstruktion in der Mengenlehre

Aussonderungsaxiom

Axiom 1.1.8 (Aussonderungsaxiom) Zu jeder Menge M und jeder eigenschaft P gibt es eine Teilmenge N von M, die gerade aus den Elementen von M mit dieser eigenschaft besteht.

Notation 1.1.9 Weitere Symbole.

$\mid$	mit der Eigenschaft:	z.b. $\{0;1;2\} = \{n \in \mathbb{N} \mid n \leq 2\}$.

Satz 1.1.10 Es gibt eine Menge, die keine Elemente enthält: Mann nennt diese Menge die **leere Menge** und bezeichnet sie mit $\emptyset$. □

Beweis. Wir behaupten, dass es mindenstens eine Menge M gibt. Dann kann man, dank dem Aussonderungsaxiom die Menge

$$\emptyset = \{x \in M \mid x \neq x\}$$

definieren. Die Menge $\emptyset$ enthält keine Elemente. ■

Bemerkung 1.1.11 Die leere Menge ist in jede Menge enthalten: für jede Menge M gilt $\emptyset \subset M$.

Satz 1.1.12 Es gibt keine Menge die jede Menge als Element enthält □

Beweis. Siehe Tutorium 1. ■

Vereinigungsaxiom

Axiom 1.1.13 (Vereinigungsaxiom)

1. Seien M und N zwei Mengen, dann gibt es eine Menge $M \cup N$, die **Vereinigung** von M und N, die genau alle Elemente von M und N enthält. Mit Symbole

$$M \cup N = \{x \mid x \in M \text{ oder } x \in N\}.$$

2. Verallgemeinerung. Sei I eine Indexmenge und $(M_i)_{i\in I}$ eine Familie von Mengen, dann gibt es eine Menge

$$\bigcup_{i\in I} M_i,$$

die **Vereinigung** von $(M_i)_{i\in I}$, die genau alle Elemente von M_i für alle $i \in I$ enthält. Mit Symbole

$$\bigcup_{i\in I} M_i = \{x \mid \text{es gibt ein } i \in I \text{ so dass } x \in M_i\}.$$

Beispiel 1.1.14 Here sind Beispiele von Mengen.

1. Die leere Menge $\emptyset$.

2. Zu jedes Element $x \in M$ kan man die einelementige Menge $\{x\}$ definieren.

2. Zu zwei Elemente x und y kann mann die Paarmenge

$$\{x, y\} = \{x\} \cup \{y\} = \{y\} \cup \{x\} = \{y, x\}$$

definieren. Es ist die Menge, die genau x und y entählt.

Aus dem Vereinigungsaxiom und dem Aussonderungsaxiom ergibt sich die Existenz des Durchschnitts von Mengen.

Satz 1.1.15 (Durchschnitt)

1. Seien M und N zwei Mengen, dann gibt es genau eine Menge $M \cap N$, der **Durchschnitt** von M und N, die genau die Elementen von M und N enthält. Mit Symbole

$$M \cap N = \{x \in M \cup M \mid x \in M \text{ und } x \in N\}.$$

2. Verallgemeinerung. Sei I eine Indexmenge und $(M_i)_{i\in I}$ eine Familie von Mengen, dann gibt es genau eine Menge

$$\bigcap_{i\in I} M_i,$$

der **Durchschnitt** von $(M_i)_{i\in I}$, welche genau die Elemente, die in jeder Menge M_i für all $i \in I$ enthalten sind. Mit Symbole

$$\bigcap_{i\in I} M_i = \left\{ x \in \bigcup_{i\in I} M_i \mid \text{für alle } i \in I \text{ gilt } x \in M_i \right\}.$$

Satz 1.1.16 Seien M, N und O drei Mengen. Dann gilt.

1. $M \cup M = M$ und $M \cap M = M$.

2. $M \cup N = N \cup M$ und $M \cap N = N \cap M$.

3. $M \cup (N \cup O) = (M \cup N) \cup O$ und $M \cap (N \cap 0) = (M \cap N) \cap O$ □

Beweis. Übung ■

Satz 1.1.17 Seien M, N und O drei Mengen. Dann gilt.

1. $M \cap (N \cup O) = (M \cap N) \cup (M \cap O)$.

2. $M \cup (N \cap O) = (M \cup N) \cap (M \cup O)$. □

Beweis. Siehe Übungsblatt 0. ■

Definition 1.1.18 Das **Komplement** von N in M ist die Menge $M \setminus N$ von elemente die in M und nich in N enthalten sind. Mit Symbole:

$$M \setminus N = \{x \in M \mid x \notin N\}.$$

Satz 1.1.19 Seien M, N und O drei Mengen. Dann gilt.

1. $M \setminus (N \cup O) = (M \setminus N) \cap (M \setminus O)$.

2. $M \setminus (N \cap O) = (M \setminus N) \cup (M \setminus O)$. □

Beweis. Siehe Übungsblatt 0. ■

Potenzmengensaxiom

Axiom 1.1.20 Sei M eine Menge, dann gibt es genau eine Menge, die **Potenzmenge** $\mathfrak{P}(M)$ von M, welche Elemente genau alle Teilmenge von M sind.

Beispiel 1.1.21

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

2. $\mathfrak{P}(\{\emptyset\}) = \{\emptyset; \{\emptyset\}\}$.

3. $\mathfrak{P}(\{0;1;2\}) = \{\emptyset; \{0\}; \{1\}; \{2\}; \{0;1\}; \{0;2\}; \{1;2\}; \{0;1;2\}\}$.

Kartesische Produkt

Definition 1.1.22 (Kartesische Produkt) Seien M und N zwei Mengen.

1. Ein **geordnetes Paar** von Elementen $x \in M$ und $y \in N$ besteht aus der Angabe eines erten Elements $x \in M$ und eines zweiten Elements $y \in N$. Paaren werden als (x, y) geschrieben.

2. Die Menge aller geordneten Paare von Elementen aus M und N heißt das **Kartesische Produkt** und ist durch $M \times N = \{(x, y) \mid x \in M,\ y \in N\}$ bezeichnet.

Satz 1.1.23 Es gilb $(x, y) = (y, x)$ genau dann wenn $x = y$. □

Beispiel 1.1.24 Sei $M = \{0;1;2\}$ und $N = \{A, B\}$ dann gilt

$$M \times N = \{(0, A); (0, B); (1, A); (1, B); (2, A); (2, B)\}.$$

1.2 Natürlische Zahlen

1.2.1 Definition

Wir haben noch keine unendlische Menge, *i.e.* Menge mit unendlischen vielen Elementen, gesehen. Wir brauchen eigentlich ein neues Axiom dafür.

Axiom 1.2.1 (Peano Axiome) Es gibt eine Menge $\mathbb{N}$, die Meger der natürlischen Zahlen mit den folgenden Eigenschaften:

- zu jeder $n \in N$, gibt es genau einen Nachfolger $N(n) \in \mathbb{N}$ (später $N(n) = n+1$).
- Es gibt ein Element $0 \in \mathbb{N}$, so dass für alle $n \in \mathbb{N}$ gilt $N(n) \neq 0$.
- Jede $n \in \mathbb{N}$ ist Nachfolger höchstens einer natürlichen Zahlen.
- Sei M eine Teilmenge von $\mathbb{N}$, so dass
  - $0 \in M$
  - $n \in M \Rightarrow N(n) \in M$

  dann gilt $M = \mathbb{N}$ (**Induktionseigenschaftaxiom**).

Notation 1.2.2 Konkret kann man die natürlische Zahlen wie folgt definieren: 0, $1 = N(0)$, $2 = N(1)$, $3 = N(2)$ ... $n + 1 = N(n)$.

Man kann mit dieser Definiton die klassische arthmetische Eigenschaften von $\mathbb{N}$ zurück finden.

Beispiel 1.2.3 Here sind weitere Beispiele von unendliche Mengen die man dank der Existenz von $\mathbb{N}$ konstruiren kann.

Die Menge der ganzen Zahlen ist $\mathbb{Z}$.
Die Mende der rationale Zahlen ist $\mathbb{Q}$.
Die Mende der reelen Zahlen ist $\mathbb{R}$.
Die Mende der komplexen Zahlen ist $\mathbb{C}$.

1.2.2 Induktion

Satz 1.2.4 Sei P eine eigenschaft die eine natürlische Zahl haben kann. Wenn $P(0)$ und $P(n) \Rightarrow P(n+1)$ wahr sind, dann ist $P(n)$ wahr für jede $n \in \mathbb{N}$. □

Beweis. Sei $M = \{n \in \mathbb{N} \mid P(n) \text{ ist wahr}\}$, dann gilt $0 \in M$ und $n \in M \Rightarrow N(n) \in M$. Vom Induktionseigenschaftaxiom folgt $M = \mathbb{N}$. ■

Beispiel 1.2.5

1. Für alle $n \in \mathbb{N}$ gilt $\quad 0+1+2+\cdots+n = \dfrac{n(n+1)}{2}$.

2. Für alle $n \in \mathbb{N}$ gilt $\quad 0^2+1^2+2^2+\cdots+n^2 = \dfrac{n(n+1)(2n+1)}{6}$.

3. Für alle $n \in \mathbb{N}$ gilt $\quad 0^3+1^3+2^3+\cdots+n^3 = \dfrac{n^2(n+1)^2}{4}$.

Beweis. 1. Sei $P(n)$ die Eigenschaft

$$0+1+2+\cdots+n = \frac{n(n+1)}{2}.$$

Dann gilt $P(0)$. Angenommen,dass $P(n)$ gilt, dann gilt

$$0+1+2+\cdots+n+(n+1) = \frac{n(n+1)}{2}+(n+1) = \frac{n^2+n+2n+2}{2} = \frac{(n+1)(n+2)}{2}.$$

2. und 3. Siehe Übungsblatt 0. ∎

1.3 Auswahlaxiom

Wir geben noch ein Axiom, das nicht von den Anderen abhängt.

Axiom 1.3.1 (Auswahlaxiom) Sei $(M_i)_{i\in I}$ ein Mengensystem so dass für jedes $i \in I$, gilt $M_i \neq \emptyset$ und für jede $i, j \in I$, gilt $M_i \cap M_j = \emptyset$. Dann gibt es eine Menge M, so dass für jedes $i \in I$ die Menge $M_i \cap M$ genau ein Element enthält.

Dieses Axiom wird später benutzt, um zu beweisen, dass jeder Vektorraum eine Basis enthält.

1.4 Abbildungen

Definition 1.4.1 Seien M und N zwei Mengen. Eine **Abbildung** f von M nach N ist eine Vorschrift, durch die jede Elemente $x \in M$ genau ein Element $f(x) \in N$ zugeordnet wird. In Symbol man schreibt:

$$\begin{array}{rccl} f: & M & \to & N \\ & x & \mapsto & f(x). \end{array}$$

Die Menge M heißt **Definitionsbereich** und N heißt **Wertebereich** der Abbildung f.

Beispiel 1.4.2

1. Sei M eine Menge, es gibt die **identische Abbildung** $\mathrm{Id}_M : M \to M$, $x \mapsto x$.

2. Sei $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto x^2$.

Definition 1.4.3 Seien $f : M \to N$ und $g : N \to O$, dann kann man f mit g **componieren**. Als Resultat erhält man eine Abbildung $g \circ f : M \to O$ definiert durch $x \mapsto g(f(x))$.

Definition 1.4.4 Sei $f : M \to N$ eine Abbildung und seien $X \subset M$ und $Y \subset N$ Teilmengen von M und N. Das **Bild** von X under f ist die Teilmenge von N defienert durch

$$f(X) = \{y \in N \mid \exists x \in X \text{ mit } y = f(x)\} = \{f(x) \mid x \in X\}.$$

Das **Urbild** von Y ist die Teilmenge von M defieniert durch

$$f^{-1}(Y) = \{x \in M \mid f(x) \in Y\}.$$

Für eine Teilmenge $\{y\}$ mit einem einzigen Element schreibt man $f^{-1}(y) = f^{-1}(\{y\})$.

Beispiel 1.4.5 Sei $f : \mathbb{Z} \to \mathbb{Z}$ die Abbildung definiert durch $x \mapsto x^2$. Dann gilt $f(\{-1; 1\}) = \{1\}$ und $f^{-1}(1) = \{-1; 1\}$.

Definition 1.4.6 Sei $f : M \to N$ eine Abbildung.

1. Die Abbildung f heißt **injektiv** wenn, für alle $x, x' \in M$ gilt die Implikazion $f(x) = f(x') \Rightarrow x = x'$ (oder $x \neq x' \Rightarrow f(x) \neq f(x')$).

2. Die Abbildung f heißt **surjektiv** wenn, $f(M) = N$.

3. Die Abbildung f heißt **bijektiv** wenn sie injektiv und surjektiv ist.

Satz 1.4.7 Sei $f : M \to N$ eine Abbildung. Die Abbildung f ist bijektiv genau dann wenn existiert eine Abbildung $g : N \to M$ mit $g \circ f = \mathrm{Id}_M$ und $f \circ g = \mathrm{Id}_N$.

Für f bijektiv ist die Abbildung g eindeutig definiert. □

Beweis. Angenomment f sei bijektiv. Sei $y \in N$. Als f surjektiv ist, existiert ein Element $x \in M$ mit $f(x) = y$. Das Element x ist von y eindeutig definiert weil für $x' \in M$ mit $f(x) = f(x')$ gilt $x = x'$. Man definiert $g : N \to M$ mit $g(y) = x$. Dann gilt $f \circ g(y) = f(g(y)) = f(x) = y$ und $g \circ f(x) = g(f(x)) = g(y) = x$.

Die Abbildung g ist eindeutig: sei $h : N \to M$ mit $h \circ f = \mathrm{Id}_M$ und $f \circ h = \mathrm{Id}_N$, dann gilt für $y = f(x) \in N$: $h(y) = g(f(x)) = x = g(y)$. Da f surjetiv gilt die Gleichheit $h(y) = g(y)$ für alle $y \in N$.

Angenommen es gibt g, dann für $x, y \in M$ mit $f(x) = f(y)$ gilt $x = g(f(x)) = g(f(y)) = y$, so dass f injektiv ist. Sei $y \in N$ dann gilt $y = f(g(y))$ und f ist surjektiv. ■

Definition 1.4.8 Sei $f : M \to N$ eine bijektive Abbildung, dann ist die einzige Abbildung g so dass $g \circ f = \mathrm{Id}_M$ und $f \circ g = \mathrm{Id}_N$ die **Umkehrabbildung** genannt und wird mit $f^{-1} : N \to M$ geschrieben.

Bemerkung 1.4.9 Sei $f : M \to N$ eine Abbildung und Y einen Teilmenge von N. Die Urbild $f^{-1}(Y)$ ist für jede (auch nicht bijektive) Abbildung definiert und für $y \in N$ ist die Urbild $f^{-1}(y)$ für jede (auch nicht bijektive) Abbildung definiert.

Satz 1.4.10 Seien $f : M \to N$ und $g : N \to O$ zwei Abbildungen. Dann gilt.

1. f und g injektiv $\Rightarrow g \circ f$ injektiv.

2. f und g surjektiv $\Rightarrow g \circ f$ surjektiv.

3. f und g bijektiv $\Rightarrow g \circ f$ bijektiv. □

Beweis. 1. Seien $x, y \in M$, so dass $g \circ f(x) = g \circ f(y)$, dann gilt $g(f(x)) = g(f(y))$ und als g injektiv ist, gilt $f(x) = f(y)$. Als f injektiv ist, gilt $x = y$ so dass $g \circ f$ injektiv ist.

2. Sei $z \in O$. Als g surjektiv ist, gibt es $y \in N$ mit $g(y) = z$. Als f sujektiv ist, gibt es $x \in M$ mit $f(x) = y$. Dann gilt $g \circ f(x) = g(f(x)) = g(y) = z$ und $g \circ f$ ist surjektiv.

3. Folgt aus 1. und 2. ■

Satz 1.4.11 Sei $f : M \to N$ eine Abbildung zwischen nicht leere Mengen.

1. Die Abbildung f ist injektiv genau dann wenn, es eine Abbildung $g : N \to M$ mit $g \circ f = \mathrm{Id}_M$ gibt.

2. Die Abbildung f ist surjektiv genau dann wenn, es eine Abbildung $h : N \to M$ mit $f \circ h = \mathrm{Id}_N$ gibt.

3. Wenn f bijektiv ist dann sind die beide Abbildungen $g : N \to M$ und $h : N \to M$ gleich die Umkehrabbildung f^{-1}. □

Beweis. Siehe Tutorium 2. ■

Definition 1.4.12 Sei $f : M \to N$ eine Abbildung, der **Graph** von f ist die Teilmenge $\Gamma(f) \subset M \times N$ von $M \times N$ definiert durch

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

Definition 1.4.13 Seien M und N zwei Mengen, dann ist N^M die **Menge aller Abbildungen** von M nach N.

1.4.1 Abbildungen und Mengenoperationen

Satz 1.4.14 Seien $f : M \to N$ eine Abbildung, $M_1, M_2 \subset M$ und $N_1, N_2 \subset N$ dann gilt:

1. $M_1 \subset M_2 \Rightarrow f(M_1) \subset f(M_2)$ und $N_1 \subset N_2 \Rightarrow f^{-1}(N_1) \subset f^{-1}(N_2)$.
2. $f(M_1 \cup M_2) = f(M_1) \cup f(M_2)$ und $f^{-1}(N_1 \cup N_2) = f^{-1}(N_1) \cup f^{-1}(N_2)$.
3. $f(M_1 \cap M_2) \subset f(M_1) \cap f(M_2)$ und $f^{-1}(N_1 \cap N_2) = f^{-1}(N_1) \cap f^{-1}(N_2)$.
4. $f(M_1) \setminus f(M_2) \subset f(M_1 \setminus M_2)$ und $f^{-1}(N_1 \setminus N_2) = f^{-1}(N_1) \setminus f^{-1}(N_2)$. □

Beweis. Siehe Übungsblatt 2. ■

1.5 Relationen

1.5.1 Erste Definition

Definition 1.5.1 Sei M eine Menge. Eine **Relation** auf der Menge M ist eine Teilmenge R von $M \times M$. Seien x, y zwei Elemente in M, für $(x, y) \in R$ schreibt man $x \sim_R y$.

Beispiel 1.5.2 1. Sei M eine Menge, die Relation $R = \{(x, y) \in M \times M \mid x = y\}$ ist die Gleichheitsrelation. Es gilt $x \sim_R y \Leftrightarrow x = y$.

2. Sei $M = \mathbb{N}$ und $R = \{(x, y) \in \mathbb{N} \times \mathbb{N} \mid x \leq y\}$. Dann ist R eine Relation auf $\mathbb{N}$.

3. Sei M eine Menge und $R = \{(A, B) \in \mathfrak{P}(M) \mid A \cap B = \emptyset\}$. Dann ist R eine Relation auf M.

Definition 1.5.3 Sei R eine Relation auf einer Menge M.

1. R heißt **reflexiv**, wenn $x \sim_R x$ für alle $x \in M$.
2. R heißt **symmetrisch**, wenn $x \sim_R y \Rightarrow y \sim_R x$.
3. R heißt **antisymmetrisch**, wenn $(x \sim_R y$ und $y \sim_R x) \Rightarrow x = y$.
4. R heißt **transitiv**, wenn $(x \sim_R y$ und $y \sim_R z) \Rightarrow x \sim_R z$.

Beispiel 1.5.4 1. Sei M eine Menge, die Gleichheitsrelation $R = \{(x, y) \in M \times M \mid x = y\}$ ist reflexiv, symmetrisch, antisymmetrisch und transitiv.

2. Sei $M = \mathbb{N}$ die Relation $R = \{(x, y) \in \mathbb{N} \times \mathbb{N} \mid x \leq y\}$ ist reflexiv, antisymmetrisch und transitiv aber nicht symmetrisch.

3. Sei M eine nichtleere Menge. Die Relation $R = \{(A, B) \in \mathfrak{P}(M) \mid A \cap B = \emptyset\}$ auf der Menge M ist nicht reflexiv, symmetrisch, nicht antisymmetrisch und nicht transitiv.

1.5.2 Ordnungsrelationen

Definition 1.5.5 Sei M eine Menge und R eine Relation auf M. Die Relation R heißt **Ordnungsrelation**, wenn R reflexiv, antisymmetrisch und transitiv ist.

Beispiel 1.5.6 1. Sei M eine Menge, die Gleichheitsrelation ist eine Ordnungsrelation.

2. Sei $M = \mathbb{N}$ die Relation $R = \{(x, y) \in \mathbb{N} \times \mathbb{N} \mid x \leq y\}$ ist eine Ordnungsrelation.

3. Sei M eine nichtleere Menge. Die Relation $R = \{(A, B) \in \mathfrak{P}(M) \mid A \cap B = \emptyset\}$ ist nicht eine Ordnungsrelation.

1.5.3 Äquivalenzrelationen

Definition 1.5.7 Sei R eine Relation auf einer Menge M. 4. R heißt **Äquivalenzrelation**, wenn R reflexiv, symmetrisch und transitiv ist.

Beispiel 1.5.8 1. Sei M eine Menge, die Gleichheitsrelation ist eine Äquivalenzrelation.

2. Sei $M = \mathbb{N}$ die Relation $R = \{(x, y) \in \mathbb{N} \times \mathbb{N} \mid x \leq y\}$ ist keine Äquivalenzrelation.

3. Sei M eine nichtleere Menge. Die Relation $R = \{(A, B) \in \mathfrak{P}(M) \mid A \cap B = \emptyset\}$ ist keine Äquivalenzrelation.

Lemma 1.5.9 Sei $R = \{(x, y) \in \mathbb{N} \times \mathbb{N} \mid x - y \text{ ist gerade}\}$. Dann ist R eine Äquivalenzrelation auf $\mathbb{N}$. □

Beweis. Siehe Übungsblatt 2. ■

Satz 1.5.10 Sei $f : M \to N$ eine Abbildung. Dann ist $R = \{(x, y) \in M \mid f(x) = f(y)\}$ eine Äquivalenzrelation. □

Beweis. Als $f(x) = f(x)$, gilt $x \sim_R x$. Für $x \sim_R y$, gilt $f(x) = f(y)$ und $f(y) = f(x)$, so dass $y \sim_R x$ gilt. Für $x \sim_R y$ und $y \sim_R z$, gilt $f(x) = f(y)$ und $f(y) = f(z)$, so dass $f(x) = f(z)$ und $x \sim_R z$ gilt. ■

1.5.4 Quotient

Definition 1.5.11 Sei R eine Äquivalenzrelation auf einer Menge M.

1. Die **Äquivalenzklasse** $[x]$ von x ist die Menge aller Elemente y mit $x \sim_R y$. Mit Symbol:

$$[x] = \{y \in M \mid x \sim_R y\}.$$

2. Die Gesamtheit der Äquivalenzklassen bildet eine Teilmenge der Potenzmenge $\mathfrak{P}(M)$ die man M/R bezeichnet und **Quotientenmenge von** M **nach** R. Mit Symbol

$$\begin{aligned} M/R &= \{N \in \mathfrak{P}(M) \mid \exists x \in M \text{ mit } N = [x]\} \\ &= \{[x] \in \mathfrak{P}(M) \mid x \in M\}. \end{aligned}$$

Lemma 1.5.12 Sei R eine Äquivalenzrelation auf einer Menge M und sei $x, y \in M$. Dann sind die folgende Aussagen äquivalent:

1. $[x] = [y]$;

2. $[x] \cap [y] \neq \emptyset$;

3. $x \sim_R y$. □

Beweis. 1. $\Rightarrow$ 2. Trivial: $x \in [x] = [y]$ also $x \in [x] \cap [y]$.

2. $\Rightarrow$ 3. Sei $z \in [x] \cap [y]$. Dann gilt $x \sim_R z$ und $y \sim_R z$. Als R symmetrisch ist gilt $z \sim_R y$ und von der transitivität gilt $x \sim_R y$.

3. $\Rightarrow$ 1. Sei $z \in [x]$, dann gilt $x \sim_R z$. Als R symmetrisch und transitiv ist gilt $y \sim_R z$ *i.e.* $z \in [y]$ und $[x] \subset [y]$. Die Inklusion $[y] \subset [x]$ kann man mit der selben Methode beweisen. ■

Korollar 1.5.13 Sei $O \in M/R$ eine Äquivalenzklasse dann gilt $x \in O \Leftrightarrow [x] = O$.

Definition 1.5.14 Sei M eine Menge, eine **Partition** von M ist eine Familie $(M_i)_{i \in I}$ von Teilmenge $M_i \subset M$ so dass

- $M_i \cap M_j = \emptyset$ für $i \neq j$,
- $\bigcup_{i \in I} M_i = M$.

Satz 1.5.15 Sei R eine Äquivalenzrelation auf einer Menge M. Dann bildet die Familie von Äquivalenzklassen eine Partition von M. □

Beweis. Aus Lemma 1.5.12 gilt $[x] \cap [y] = \emptyset$ für $[x] \neq [y]$. Außerdem, gibt es für jedes Element $x \in M$ eine Klasse: $[x]$ so dass $x \in [x]$. Es gilt daher

$$M \subset \bigcup_{[x] \in M/R} [x].$$

Die umgekehrte Inklusion gilt auch da $[x] \subset M$ für alle $[x]$. ∎

Definition 1.5.16 Sei R eine Äquivalenzrelation auf einer Menge M. Die Abbildung $p_R : M \to M/R$ defieniert durch $x \mapsto [x]$ heißt die **kanonische Projektion**.

Lemma 1.5.17 Sei R eine Äquivalenzrelation auf einer Menge M.

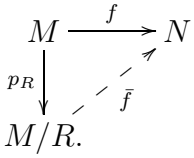
1. Die kanonische Projektion p_R ist surjektiv.

2. Es gilt für $x, y \in M$: $[x] = [y] \Leftrightarrow p_R(x) = p_R(y)$. □

Beweis. 1.Sei $[x] \in M/R$, dann gilt $[x] = p_R(x)$.

2. Trivial aus der Definition. ∎

Satz 1.5.18 Sei R eine Äquivalenzrelation auf einer Menge M. Sei $f : M \to N$ eine Abbildung, so dass $[x] = [y] \Rightarrow f(x) = f(y)$. Dann gibt es eine Abbildung $\bar{f} : M/R \to N$, so dass $f = \bar{f} \circ p_R$.



Beweis. M/R ist eine Menge von Teilmengen von M. Sei $O \in M/R$ (z.b. $O = [z]$ für $z \in M$). Wenn die Abbildung $\bar{f}$ existiert, dann gilt für $x \in O$: $f(x) = \bar{f}(p_R(x)) = \bar{f}([x]) = \bar{f}(O)$ *i.e.* $\bar{f}(O) = f(x)$.

Seien $x, y \in O$, dann gilt aus Lemma 1.5.17: $[x] = O = [y]$ und $f(x) = f(y)$. Die Abbildung $O \to N$ definiert durch $x \mapsto f(x)$ ist konstant gleich $n \in N$. Wir definieren $\bar{f}(O) = n$. Es gilt $n = f(x)$ für jeder $x \in O$.

Es gilt $\bar{f} \circ p_R(x) = \bar{f}([x]) = f(x)$. ∎

2 Gruppen, Körper und Ringe

2.1 Gruppen

2.1.1 Definition und Beispiele

Definition 2.1.1 Eine **Gruppe** ist ein geordnetes Paar (G, m) mit G einer Menge und m einer Abbildung $m : G \times G \to G$ (auch **Verknüpfung** gennant) so dass die folgenden Eigenschaften erfüllt sind:

- Es existiert ein **neutrales Element** e in G mit $m(e, x) = m(x, e) = x$ für alle $x \in G$.
- Die Verknüpfung m ist **assoziativ**, dass heißt $m(x, m(y, z)) = m(m(x, y), z)$ für alle $x, y, z \in G$.
- Für jedem $x \in G$ gibt es ein **inverses Element**, dass heißt eine Element $y \in G$ mit $m(x, y) = m(y, x) = e$.

Definition 2.1.2 Eine Gruppe (G, m) heißt **kommutativ** oder **abelsch** falls gilt: $m(x, y) = m(y, x)$ für alle $x, y \in G$.

Notation 2.1.3 Wir werden oft die Verknüpfung $m : G \times G \to G$ mit einem multiplikativen Symbol schreiben: $m(x, y) = x \cdot y$. Die Axiome für die Definition einer Gruppen sehen wie folgt aus:

- **Neutrales Element**: $e \in G$ mit $e \cdot x = x \cdot e = x$ für alle $x \in G$.
- **Associativität**: $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ für alle $x, y, z \in G$.
- **Inverses Element**: für jedem $x \in G$ existiert $y \in G$ mit $x \cdot y = y \cdot x = e$.

Die **Kommutativität** sieht wie folgt aus:

$$x \cdot y = y \cdot x.$$

Beispiel 2.1.4 Hier sind Beispiele von Gruppen:

- $(\mathbb{Z}, +)$, wo $+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ durch $(x, y) \mapsto x + y$ definiert ist, ist eine abelsche Gruppe.

- $(\mathbb{Q}, +)$, wo $+ : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$ durch $(x, y) \mapsto x + y$ definiert ist, ist eine abelsche Gruppe.
- $(\mathbb{R}, +)$, wo $+ : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ durch $(x, y) \mapsto x + y$ definiert ist, ist eine abelsche Gruppe.
- $(\mathbb{C}, +)$, wo $+ : \mathbb{C} \times \mathbb{C} \to \mathbb{C}$ durch $(x, y) \mapsto x + y$ definiert ist, ist eine abelsche Gruppe.
- $(\mathbb{Q} \setminus \{0\}, \times)$, wo $\times : \mathbb{Q} \setminus \{0\} \times Q \setminus \{0\} \to \mathbb{Q} \setminus \{0\}$ durch $(x, y) \mapsto x \times y$ definiert ist, ist eine abelsche Gruppe.
- Für eine Menge M, die Menge $\mathrm{Bij}(M)$ der bijektiven Selbstabbildungen $f : M \to M$ mit der Verknüpfung $\mathrm{Bij}(M) \times \mathrm{Bij}(M) \to \mathrm{Bij}(M)$ gegeben durch Komposition von Abbildungen: $(f, g) \mapsto f \circ g$ ist eine Gruppe. Die Gruppe $(\mathrm{Bij}(M), \circ)$ ist nicht kommutativ sofern M mindestens drei paarweise vershiedene Elemente enthält.
- $(\mathbb{N}, +)$ ist keine Gruppe: 1 hat kein inverses Element.

Satz 2.1.5 Sei $(G, \cdot)$ eine Gruppe.

1. Das neutral Element ist eindeutig bestimmt.

2. Sei $x \in G$, das inverse Element von x ist eindeutig bestimmt. □

Beweis. 1. Seien e und e' zwei neutrale Elemente. Dann gilt $e' = e \cdot e'$ weil e' neutral ist und $e \cdot e' = e'$ weil e neutrql ist. Es folgt $e' = e \cdot e' = e$.

2. Seien y und y' zwei inverse Elemente von x. Dann gilt

$$y = e \cdot y = (y' \cdot x) \cdot y = y' \cdot (x \cdot y) = y'.$$

Beispiel 2.1.6 Wir beschreiben das neutral Element und das inverse von einem Element x in den obigen Beispielen von Gruppen.

- $(\mathbb{Z}, +)$: neutral Element 0. Inverse von x: $-x$.
- $(\mathbb{Q}, +)$: neutral Element 0. Inverse von x: $-x$.
- $(\mathbb{R}, +)$: neutral Element 0. Inverse von x: $-x$.
- $(\mathbb{C}, +)$: neutral Element 0. Inverse von x: $-x$.
- $(\mathbb{Q} \setminus \{0\}, \times)$: neutral Element 1. Inverse von x: $\frac{1}{x} = x^{-1}$.
- $(\mathrm{Bij}(M), \circ)$: neutral Element Id_M. Inverse von f: f^{-1}.

Notation 2.1.7

1. Oft (aber nicht immer) werden wir allgemeine Verknüpfungen auf G die eine Gruppe definieren mit $\cdot$ bezeichnen. In diesem Fall werden wir das neutral Element mit 1 bezeichnen und das inverse Element von x mit x^{-1} bezeichnen.

2. Wenn eine Gruppe abelsch ist werden wir oft (aber nicht immer) die Verknüpfung mit $+$ bezeichnen. Dann werden wir das neutral Element mit 0 bezeichnen und das inverse Element von x mit $-x$ bezeichnen.

3. Sei $(G, \cdot)$ eine Gruppe und seien $(a_i)_{i\in[1,n]}$ n Elemente in G. Dann werden wir das Produkt von diesen Elementen mit

$$\prod_{i=1}^{n} a_i$$

bezeichnen. Falls $n = 0$ zugelassen ist, dann handelt es sich um die **leere Folge**. Man erklärt das zugehörige leere Produkt durch

$$\prod_{i=1}^{0} a_i = 1.$$

4. Sei $(G, +)$ eine Gruppe und seien $(a_i)_{i\in[1,n]}$ n Elemente in G. Dann werden wir die Somme von diesen Elementen mit

$$\sum_{i=1}^{n} a_i$$

bezeichnen. Falls $n = 0$ zugelassen ist, dann handelt es sich um die **leere Folge**. Man erklärt das zugehörige leere Somme durch

$$\sum_{i=1}^{0} a_i = 0.$$

2.1.2 Untergruppe

Definition 2.1.8 Sei $(G, \cdot)$ eine Gruppe und $H \subset G$ eine Teilmenge, dann heißt H eine **Untergrupp** von G wenn gilt:

1. $1 \in H$,
2. $x, y \in H \Rightarrow x \cdot y \in H$,
3. $x \in H \Rightarrow x^{-1} \in H$.

Satz 2.1.9 Sei H eine Untergrupe von $(G, \cdot)$, dann ist $(H, \cdot)$ eine Gruppe. □

Beweis. Siehe Übungsblatt 3. ∎

Satz 2.1.10 Sei $(G, \cdot)$ eine Gruppe und seien x, y, z Elemente in G. Dann gilt:

1. $xy = xz \Rightarrow y = z$,
2. $yx = zx \Rightarrow y = z$,
3. $(x^{-1})^{-1} = x$,
4. $(xy)^{-1} = y^{-1}x^{-1}$. □

Beweis. 1. Es gilt $y = (x^{-1}x)y = x^{-1}(xy) = x^{-1}(xz) = (x^{-1}x)z = z$.

2. Es gilt $y = y(xx^{-1}) = (yx)x^{-1} = (zx)x^{-1} = z(xx^{-1}) = z$.

3. Es gilt $xx^{-1} = x^{-1}x = 1$, das heißt x ist das inverse Element für x^{-1}.

3. Es gilt $(xy)(y^{-1}x^{-1}) = x(yy^{-1})x^{-1} = xx^{-1} = 1$ und $(y^{-1}x^{-1})xy = y^{-1}(x^{-1}x)y = y^{-1}y = 1$, das heißt $y^{-1}x^{-1}$ ist das inverse Element für xy. ∎

2.1.3 Gruppenhomomorphismus

Definition 2.1.11 Seien $(G, \cdot)$ und $(G', \star)$ Gruppen. Eine Abbildung $f : G \to G'$ heißt **Gruppenhomomorphismus** wenn für jeden $x, y \in G$ gilt:

$$f(xy) = f(x) \star f(y).$$

Satz 2.1.12 Sei $f : G \to G'$ ein Gruppenhomomorphismus dann gilt für alle $x \in G$

$$f(1) = e_{G'} \text{ und } f(x^{-1}) = f(x)^{-1}.$$

wo 1 das neutral Element von G ist und $e_{G'}$ das neutral Element von G' ist. □

Beweis. Es gilt $f(1) \star f(1) = f(1 \cdot 1) = f(1) = f(1) \star e_{G'}$ und von Satz 2.1.10.1 folgt $f(1) = e_{G'}$.

Es gilt $f(x) \star f(x^{-1}) = f(xx^{-1}) = f(1) = e_{G'}$ und $f(x^{-1}) \star f(x) = f(x^{-1}x) = f(1) = e_{G'}$, dass heißt $f(x^{-1})$ ist das inverse Element von $f(x)$. ∎

Satz 2.1.13 Sei $f : G \to G'$ ein Gruppenhomomorphismus, dann ist $\ker(f) = \{x \in G \mid f(x) = e_{G'}\}$ eine Untergruppe von G. □

Beweis. Es gilt $1 \in \ker(f)$. Für $x, y \in \ker(f)$ gilt $f(xy) = f(x) \star f(y) = e_{G'} \star e_{G'} = e_{G'}$, dass heißt $xy \in \ker(f)$ und $f(x^{-1}) = f(x)^{-1} = e_{G'}^{-1} = e_{g'}$ dass heißt $x \in \ker(f)$. ∎

Definition 2.1.14 Sei $f : G \to G'$ ein Gruppenhomomorphismus, dann heißt die Untergruppe $\ker(f) = \{x \in G \mid f(x) = e_{G'}\}$ der **Kern** von f.

Satz 2.1.15 Sei $f.G \to G'$ ein Gruppenhomomorphismus. Die Abbildung f ist genau dann injektiv, wenn $\ker(f) = \{1\}$. □

Beweis. Angenommen f sei injektiv, dann gilt für $x \in \ker(f)$: $f(x) = e_{G'} = f(1)$ und $x = 1$ folgt von der Injektivität.

Angenommen $\ker(f) = \{1\}$, dann gilt für $x, y \in G$ mit $f(x) = f(y)$: $f(xy^{-1}) = f(x)f(y)^{-1} = f(x)f(x)^{-1} = e_{G'}$, dass heißt $xy^{-1} \in \ker(f)$. Weiter folgt $xy^{-1} = 1$ und $x = y$. ■

Satz 2.1.16 Sei $f : G \to G'$ ein Gruppenabbildung, dann ist das Bild von f eine Untergruppe von G' □

Beweis. Siehe Übungsblatt 3. ■

2.2 Körper

2.2.1 Definition und Beispiele

Definition 2.2.1 Ein **Körper** ist ein geordnetes Paar $(K, +, \cdot)$ mit K einer Menge und $+$, $\cdot$ Verknüpfungen auf K, so dass die folgenden Eigenschaften erfüllt sind:

- $(K, +)$ ist eine kommutative Gruppe mit neutral Element 0.
- $(K \setminus \{0\}, \cdot)$ ist eine kommutative Gruppe mit neutral Element 1.
- Für jeden $x, y, z \in K$ gilt $x(y + z) = xy + xz$ (**Distributivgesetzt**).

Das Element 0 heißt das **Nullelement** von K und das Element 1 heißt das **Einselement** von K.

Notation 2.2.2

1. In die Gleichung $x(y + z) = xy + xz$ hätten Wir eigentlich $x(y + z) = (xy) + (xz)$ schreiben mussen. Implizit hier ist, dass die Multiplication $\cdot$ Vorrang der Addition $+$ hat.

2. Wir schreiben $K^\times$ für $K \setminus \{0\}$.

3. Für $x \in K$ und $y \in K^\times$ schreiben wir $\dfrac{x}{y} = xy^{-1}$.

Beispiel 2.2.3 Hier sind Beispiele von Körper:

- $(\mathbb{Q}, +, \cdot)$ ist einer Körper.
- $(\mathbb{R}, +, \cdot)$ ist einer Körper.
- $(\mathbb{C}, +, \cdot)$ ist einer Körper.

- $(\mathbb{Z}, +, \cdot)$ ist keiner Körper: 2 hat kein inverses Element.

Satz 2.2.4 Sei $(K, +, \cdot)$ ein Körper.

1. Es gilt $(y + z)x = yx + zx$ für alle $x, y, z \in K$,

2. Es gilt $x0 = 0x = 0$ für alle $x \in K$,

3. Es gilt $\frac{x}{y} + \frac{z}{t} = \frac{xt + yz}{yt}$ für alle $x, z \in K$ und $y, t \in K^\times$.

4. Seien $x, y \in K$, dann gilt $xy = 0_K \Rightarrow x = 0_K$ oder $y = 0_K$. □

Beweis. 1. Es gilt $(y + z)x = z(y + z) = xy + xz = yx + zx$.

2. Es gilt $0x = x0 = x(0 + 0) = x0 + x0$ und mit Satz 2.1.10.1 gilt $0x = x0 = 0$.

3. Es gilt

$$\begin{aligned}\frac{x}{y} + \frac{z}{t} &= xy^{-1} + zt^{-1} = xtt^{-1}y{-}1 + zyy^{-1}t^{-1} = xt(yt)^{-1} + yz(yt)^{-1} \\ &= (xt + yz)(yt)^{-1} = \frac{xt + yz}{yt}.\end{aligned}$$

4. Seien $x, y \in K$, mit $xy = 0_K$. Falls $x \neq 0_K$, dann gilt $y = (x^{-1}x)y = x^{-1}(xy) = x^{-1}0_K = 0_K$. ■

2.2.2 Teilkörper

Definition 2.2.5 Sei $(K, +, \cdot)$ ein Körper $L \subset K$ eine Teilmenge, dann heißt K ein **Teilkörper** von K wenn L eine Untergruppe von $(K, +)$ ist und $L^\times$ eine Untergruppen von $(K^\times, \cdot)$ ist.

Satz 2.2.6 Sei L ein Teilkörper von $(K, +, \cdot)$, dann ist $(L, +, \cdot)$ ein Körper. □

Beweis. Folgt von Satz 2.1.9. ■

Beispiel 2.2.7

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

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

3. $\mathbb{Q}(\sqrt{2}) = \{x + y\sqrt{2} \in \mathbb{R} \mid x, y \in \mathbb{Q}\}$ ist ein Teilkörper von $\mathbb{R}$ (siehe Übungsblatt 3).

2.2.3 Körperhomomorphismus

Definition 2.2.8 Seien $(K, +, \cdot)$ und $(K', +, \cdot)$ zwei Körper. Eine Abbildung $f : K \to K'$ heißt **Körperhomomorphismus** wenn $f : (K, +) \to (K', +)$ und $f : (K\times, \cdot) \to (K'^{\times}, \cdot)$ Gruppenhomomorphismus sind.

Satz 2.2.9 Sei $f : K \to K'$ ein Körperhomomorphismus dann gilt für alle $x \in K$ und $y \in K^{\times}$:

$$f(0_K) = 0_{K'},\ f(1_K) = 1_{K'}\ f(-x) = -f(x) \text{ und } f(y^{-1}) = f(y)^{-1}.$$

Beweis. Folgt von Satz 2.1.12. ∎

Beispiel 2.2.10 Sei $f : \mathbb{C} \to \mathbb{C}$ mit $f(z) = \bar{z}$ die komplexe Konjugation, dann ist f ein Körperhomomorphismus (siehe Übungsblatt 3).

Satz 2.2.11 Sei $f : K \to K'$ ein Körperhomomorphismus, dann ist f injektiv. □

Beweis. Wir berechnen $\ker(f) = \{x \in K \mid f(x) = 0_{K'}\}$. Sei $x \in \ker(f)$ mit $x \neq 0_K$, dann gilt $0_{K'} \neq 1_{K'} = f(1_K) = f(xx^{-1}) = f(x)f(x^{-1}) = 0_{K'}f(x^{-1}) = 0_{K'}$ ein Widerspruch. Weiter folgt $x \in \ker(f) \Rightarrow x = 0_K$ und $\ker(f) = \{0_K\}$ und aus Satz 2.1.15 folgt, dass f injektiv ist. ∎

2.2.4 Die Characteristik eines Körper

Definition 2.2.12 Sei K ein Körper, $n \in \mathbb{N}$ und $x \in K$. Man definiert $n \cdot x$ durch

$$n \cdot x = \underbrace{x + x + \cdots + x}_{n \text{ mal}}.$$

Man definiert $\mathrm{char}(K)$, die **Charakteristik** von K, durch $\mathrm{char}(K) = 0$ falls $n\cdot 1_K \neq 0$ für alle $n \neq 0$, und $\mathrm{char}(K) = \min\{n \in \mathbb{N} \setminus \{0\} \mid n \cdot 1_K = 0_K\}$ andernfalls.

Satz 2.2.13 Sei K ein Körper, dann gilt $\mathrm{char}(K) = 0$ oder $\mathrm{char}(K)$ ist eine Primzahl. □

Beweis. Angenommen dass $\mathrm{char}(K) \neq 0$, seien $n, m \in \mathbb{N}$ mit $\mathrm{char}(K) = nm$. Dann gilt $\mathrm{char}(K) \cdot 1_K = (nm) \cdot 1_K = (n \cdot 1_K)(m \cdot 1_K)$ und aus Satz 2.2.4 folgt $n \cdot 1_K = 0_K$ und $m \cdot 1_K = 0_K$. Aus der Definition folgt $\mathrm{char}(K) = n$ oder $\mathrm{char}(K) = m$, dass heißt $\mathrm{char}(K)$ ist eine Primzahl. ∎

2.3 Ringe

2.3.1 Definition und Beispiele

Definition 2.3.1 Ein **Ring** ist ein geordnetes Paar $(R, +, \cdot)$ mit R einer Menge und $+, \cdot$ Verknüpfungen so dass die folgenden Eigenschaften erfüllt sind:

- $(R, +)$ ist eine kommutative Gruppe,
- es existiert ein **Einselement** 1_R in R mit $1_R \cdot x = x \cdot 1_R = x$ für alle $x \in R$,
- die Verknüpfung $\cdot$ ist associativ,
- für jeden $x, y, z \in R$ gilt $x(y + z) = xy + xz$ und $(y + z)x = yx + zx$.

Definition 2.3.2 Ein Ring $(R, +, \cdot)$ heißt **kommutativ** falls gilt: $xy = yx$ für alle $x, y \in R$

Beispiel 2.3.3 Hier sind Beispiele von Ringe:

- $(\mathbb{Z}, +, \cdot)$, ist ein kommutativer Ring.
- Ein Körper $(K, +, \cdot)$ ist ein kommutativer Ring also sind $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ und $(\mathbb{C}, +, \cdot)$ kommutative Ringe.

2.3.2 Unterringe

Definition 2.3.4 Sei $(R, +, \cdot)$ ein Ring und $S \subset R$ eine Teilmenge, dann heißt S eine **Unterring** von R wenn gilt:

1. $(S, +)$ ist eine Untergrupe von $(R, +)$,
2. $x, y \in S \Rightarrow xy \in S$.
3. $1 \in S$.

Satz 2.3.5 Sei S ein Unterring von $(R, +, \cdot)$, dann ist $(S, +, \cdot)$ ein Ring. □

Beweis. Übung. ■

2.3.3 Ringhomomorphismus

Definition 2.3.6 Seien $(R, +, \cdot)$ und $(R', +, \cdot)$ Ringe. Eine Abbildung $f : R \to R'$ heißt **Ringhomomorphismus** wenn gilt:

1. $f : (R, +) \to (R', +)$ ist ein Gruppenhomomorphismus.

2. $f(1_R) = 1_{R'}$.

3. $f(xy) = f(x)f(y)$ für jeden $x, y \in R$.

Beispiel 2.3.7

1. Eine Körperhomomorphismus ist ein Ringhomomorphismus.

2. Sei K ein Körper, die Abbildung $\mathbb{Z} \to K$ definiert durch $n \mapsto n \cdot 1_K$ ist ein Ringhomomorphismus.

2.3.4 Die Ringe $\mathbb{Z}_n$

Lemma 2.3.8 (Schulwissen) Seien $x, n \in \mathbb{Z}$, mit $n \neq 0$. Dann existieren eindeutig bestimmte Elemente $r, q \in \mathbb{Z}$ mit $0 \leq r < n$ und $x = qn + r$.

Setze $r_n(x) = r$. □

Definition 2.3.9 Sei $n \in \mathbb{N}$ mit $n \geq 2$ und sei $\mathbb{Z}_n = \{0, 1, 2, \cdots, n-1\}$. Für $x, y \in \mathbb{Z}_n$ sei $x + y = r_n(x + y)$ und $x \cdot y = r_n(xy)$.

Satz 2.3.10 $(\mathbb{Z}_n, +, \cdot)$ ist ein kommutativer Ring. □

Beweis. Übung. ■

Satz 2.3.11 $(\mathbb{Z}_n, +, \cdot)$ ist ein Körper genau dann wenn n eine Primzahl ist. □

Beweis. Es gilt $n \cdot 1_{\mathbb{Z}_n} = 0_{\mathbb{Z}_n}$ und $m \cdot 1_{\mathbb{Z}_n} \neq 0_{\mathbb{Z}_n}$ für $0 < m < n$. Falls $\mathbb{Z}_n$ ein Körper ist, gilt $\text{char}(\mathbb{Z}_n) = n$ und n ist eine Primzahl.

Angenommen, dass n eine Primzahl ist, wir beweisen, dass jedem $x \in \mathbb{Z}_n \setminus \{0_{\mathbb{Z}_n}\}$ ein inverses Element hat. Wir zeigen zuerst ein Lemma.

Lemma 2.3.12 Sei n eine Primzahl ist. Dann ist $\mathbb{Z}_n$ Nullteilerfrei, dass heißt: für $x, y \in \mathbb{Z}_n$ mit $x \cdot y = 0_{\mathbb{Z}_n}$ gilt $x = 0_{\mathbb{Z}_n}$ oder $y = 0_{\mathbb{Z}_n}$. □

Beweis. Seien $x, y \in \mathbb{Z}_n$ mit $x \cdot y = 0_{\mathbb{Z}_n}$. Dann ist xy ist durch n teilbar. Da n eine Primzahl ist , folgt: n teilt x oder y. Damit ist aber $x = 0$ oder $y = 0$, da $0 \leq x, y \leq n - 1$. ■

Sei nun $x \in \mathbb{Z}_n \setminus \{0_{\mathbb{Z}_n}\}$. Definiere eine Abbildung $m_x : \mathbb{Z}_n \to \mathbb{Z}_n$ durch $m_x(y) = x \cdot y$. Dann ist m_x injektiv: seien y, z mit $m_x(y) = m_x(z)$, es folgt $x(y - z) = 0_{\mathbb{Z}_n}$. Vom Lemma folgt $y - z = 0_{\mathbb{Z}_n}$ und $y = z$.

Alle Elemente $m_x(0), m_x(1), m_x(2), \cdot, m_x(n-1)$ sind paarweise verschieden. Es sind dann n Elemente im Bild $m_x(\mathbb{Z}_n)$ von m_x. Da $\mathbb{Z}_n$ genau n Elemente hat gilt: m_x ist surjektiv. Insbesondere gilt: es gibt ein $y \in \mathbb{Z}_n$ mit $m_x(y) = 1_{\mathbb{Z}_n}$. Dann ist y das invrses Element von x und $\mathbb{Z}_n$ ist ein Körper. ∎