# Gruppen und deren Anwendungen in der Zahlentheorie
# Bad Doberan

Thomas Krakow

15.10.2006

# Inhaltsverzeichnis

# 1 Mengen und Abbildungen

## 1.1 Mengen

Oft möchte man Dinge zusammenfassen die eine bestimmte Eigenschaft besitzen. In der Mathematik fasst man diese Dinge zu einer Menge zusammen. Man spricht dann von der Menge aller Dreiecke in der Ebene oder der Menge aller durch 17 teilbaren Zahlen. Nun muss man noch genauer sagen was eine Menge überhaupt ist. Es muss also eine Definition gegeben werden. Dies ist leider nicht ganz einfach, da es bei vielen Versuchen Mengen zu definieren zu Widersprüchen kommt. Wir wählen die Definition von Cantor.

**Definition 1** *Eine Menge ist eine Zusammenfassung bestimmter, wohlunterschiedlicher Dinge unserer Anschauung oder unseres Denkens, welche Elemente der Menge genannt werden, zu einem Ganzen.*

Diese Definition führt zu Widersprüchen wie wir später sehen werden. Man kann sich eine Menge am besten als einen Sack vorstellen der irgendwelche Dinge enthält. Ist ein Ding, wir nennen es mal $x$ in diesem Sack (Menge), wir nennen ihn $M$, enthalten, so sagt man $x$ ist ein Element von $M$ und schreibt

$$x \in M.$$

Es gibt verschiedene Möglichkeiten zu sagen was in einer Menge enthalten ist. Sei $M$ unsere Menge und sie soll die Zahlen $1, 5, 7, 9$ enthalten. Man schreibt es dann folgendermaßen

$$M = \{1; 5; 7; 9\}$$

Die Dinge die in die Menge hineinkommen setzt man in geschweifte Klammern. Eine Menge enthält jedes Element höchstens einmal, d.h. die Mengen $\{1; 2; 2\}$ ist die selbe wie $\{1; 2\}$. Es kann auch vorkommen, dass in der Menge $M$ gar kein Element enthalten ist (zu vergleichen mit einem leeren Sack), man sagt dann, dass die Menge leer ist und schreibt

$$M = \emptyset.$$

Es ist auch möglich, dass Mengen andere Mengen enthalten, z.B. ist
$M = \{\{1; 2; 3\}; \{a; b\}; \{\clubsuit; \spadesuit; \heartsuit; \diamondsuit\}\}$ selbst wieder eine Menge. Bei der folgenden Menge ist aber Vorsicht geboten, $M = \{\emptyset\}$ ist die Menge die die leere Menge enthält und $M$ ist dabei selbst nicht leer. Wir müssen noch definieren wann zwei Mengen gleich sind.

**Definition 2** *Zwei Mengen sind genau dann gleich, wenn ihre Elemente gleich sind.*

Es ist beispielsweise

$$\{1;2;3\} = \{1;1;2;2;3\}; \quad \{a;b;1\} = \{1;b;a\}; \quad \{a;1\} \neq \{aa;1\}.$$

## 1.2 Teilmengen, Vereinigungen, Durchschnitte von Mengen

Wir wissen nun was Mengen sind. Bisher können wir mit den Mengen aber noch nicht so richtig arbeiten. Wir müssen aus Mengen irgendwie neue Mengen gewinnen. Um später die Arbeit zu erleichtern führen wir neue Symbole ein. Oft benutzen wir das Wort "und" wir schreiben in Zukunft dafür kurz $\wedge$, für "oder" schreiben wir $\vee$ und für "daraus folgt" schreiben wir $\Rightarrow$. Wir können nun Teilmengen von Mengen definieren.

**Definition 3 (Teilmenge)** *Eine Menge $A$ ist eine Teilmenge einer Menge $B$ falls,*

$$x \in A \Rightarrow x \in B$$

*gilt. Man schreibt dann auch $A \subset B$ oder auch $A \subseteq B$.*

Die Schreibweise $x \in A \Rightarrow x \in B$ bedeutet wörtlich übersetzt: wenn $x$ in $A$ ist so folgt daraus auch, dass $x$ in $B$ ist. Eine Menge $A$ ist also genau dann Teilmenge einer Menge $B$, wenn jedes Element welches aus in $A$ ist auch in $B$ ist. Es ist $\{1;2;3\} \subset \{1;2;3;4\}$ aber $\{1;2;3\} \not\subset \{2;3;4\}$
Es gilt immer

$$\emptyset \subset M$$

für jede Menge $M$.
Mit den neu eingeführten Symbolen können wir nun auch Mengen anders definieren. Wir können einmal die Elemente einer Menge aufzählen wie bei $A = \{1;2;3;4;5;6\}$. Wir können aber auch die Elemente einer Menge durch ihre Eigenschaften beschreiben. Die Menge $M = \{x : 1 \leq x \leq 10\}$ ist die Menge aller Zahlen zwischen 1 und 10. Der Teil $x$ : in der Mengenklammer bedeutet " alle $x$ mit der Eigenschaft ... " . Anstatt einen Doppelpunkt kann man auch einen senkrechten Strich "|" schreiben, das würde dann folgendermaßen aussehen: $M = \{x|1 \leq x \leq 10\}$.

**Definition 4 (Potenzmenge)** *Sei $M$ eine Menge, die Potenzmenge $\mathcal{P}(M)$ ist die Menge*

$$\mathcal{P}(M) = \{A : A \subset M\}.$$

Die Potenzmenge ist also die Menge aller Teilmengen einer Menge. Beispielsweise sei $M = \{a;b;c\}$, dann ist $\mathcal{P}(M) = \{\emptyset;\{a\};\{b\};\{c\};\{a;b\};\{a;c\};\{b;c\};\{a;b;c\}\}$ Für die Potenzmenge einer Menge findet man auch häufig die Bezeichnung $2^M$.

**Definition 5 (Vereinigung)** *Seien $A$ und $B$ Mengen, dann ist*

$$A \cup B = \{x : x \in A \vee x \in B\}$$

*die Vereinigung der beiden Mengen.*

Die Vereinigung zweier Mengen $A, B$ ist also die Menge aller Elemente die in $A$ oder in $B$ enthalten sind. Es ist Beispielsweise $\{1;2;3;4\} \cup \{3;4;5;6\} = \{1;2;3;4;5;6\}$.

**Definition 6 (Durchschnitt)** *Seien $A$ und $B$ Mengen, dann ist*

$$A \cap B = \{x : x \in A \wedge x \in B\}$$

*der Durchschnitt der beiden Mengen.*

Der Durchschnitt zweier Mengen $A, B$ ist also die Menge der Elemente die sowohl in $A$ als auch in $B$ enthalten sind. Es ist Beispielsweise $\{1;2;3;4\} \cap \{3;4;5;6\} = \{3;4\}$.

**Definition 7 (Differenz)** *Seien $A$ und $B$ Mengen, dann ist*

$$A \setminus B = \{x : x \in A \wedge x \notin B\}$$

*die Differenz der beiden Mengen.*

Man bildet die Differenz $A \setminus B$ also indem man aus $A$ alle Elemente raus nimmt die in $B$ enthalten sind. Beispielsweise ist $\{1;2;3;4\} \setminus \{3;4;5;6\} = \{1;2\}$.

**Beispiele:**

- $\{x : x \text{ ist Primzahl } \} \cap \{x : x \text{ ist gerade } \} = \{2\}$
- $\{x : x \text{ ist Primzahl} \Rightarrow x + 2 \text{ ist Primzahl } \} \cap \{x : 0 \leq x \leq 10\} = \{3;5\}$
- $\{x : 10 \leq x \leq 20\} \setminus \{x : x \geq 15\} = \{x : 10 \leq x < 15\}$
- $A \subset B \Rightarrow A \cup B = B \wedge A \cap B = A \wedge A \setminus B = \emptyset$
- $\{x : 5|x \wedge 6|x\} = \{x : 30|x\}$
- Sei $M_a = \{x : a|x\}$, dann ist $M_a \cap M_b = \{x : a|x \wedge b|x\} = \{x : kgV(a,b)|x\} = M_{kgV(a,b)}$

## 1.3 Klassifizierung der Zahlen

Bei späteren arbeiten mit Mengen wird es unumgänglich zu sagen welche Zahlen man meint. Es kann vorkommen, dass man nur Zahlen der Form $1; 2; 3; \ldots$ in einer Menge zulassen möchte oder auch Zahlen der Form $1.123; 3.364564356; \sqrt{2}$ zulassen möchte. Wir müssen deshalb die verschiedenen Zahlenarten unterteilen.

**Definition 8** *Die Menge*

$$\mathbb{N} = \{0; 1; 2; 3; \ldots\}$$

*heißt die Menge der natürlichen Zahlen. Sie wird mit* $\mathbb{N}$ *bezeichnet.*
*Die Menge*

$$\mathbb{Z} = \{-3; -2; -1; 0; 1; 2; 3; \ldots\}$$

*heißt die Menge der ganzen Zahlen. Sie wird mit* $\mathbb{Z}$ *bezeichnet.*

Offensichtlich ist $\mathbb{N} \subset \mathbb{Z}$. Nun können wir beispielsweise für die Menge $M = \{1; 2; 3; 4; 5\}$ auch schreiben $M = \{x : x \in \mathbb{N} \wedge 1 \leq x \leq 5\}$. Die Mengen $\mathbb{N}$ und $\mathbb{Z}$ sind offensichtlich unendlich [1] Nun müssen wir noch die "Kommazahlen" klassifizieren.

**Definition 9** *Die Menge*

$$\mathbb{Q} = \{\frac{x}{y} : x \in \mathbb{Z} \wedge y \in \mathbb{N} \setminus \{0\}\}$$

*heißt die Menge der rationalen Zahlen. Sie wird mit* $\mathbb{Q}$ *bezeichnet.*
*Die Menge*

$$\mathbb{R} = \{x : x \in \mathbb{Z} \vee x \text{ ist eine Kommazahl}\}$$

*heißt die Menge der reellen Zahlen. Sie wird mit* $\mathbb{R}$ *bezeichnet.*

Die rationalen Zahlen sind also die ganzen Zahlen zusammen mit allen Zahlen die als Bruch geschrieben werden können. Der Rest ist sind die reellen Zahlen. Warum unterscheidet man aber rationale Zahlen und reelle Zahlen? Es kann doch auch sein, dass $\mathbb{Q} = \mathbb{R}$ ist. Es kann aber ganz leicht eine Zahl angegeben werden die reell aber nicht rational ist. Eine solche Zahl ist $\sqrt{2}$. Wir wollen diese Aussage noch begründen. Angenommen es sei $\sqrt{2} \in \mathbb{Q}$, dann existieren $x \in \mathbb{Z}, y \in \mathbb{N} \setminus \{0\}$ mit $\sqrt{2} = \frac{x}{y}$, wobei der Bruch schon gekürzt ist. Es müsste dann

$$2 = \frac{x^2}{y^2} \Rightarrow 2y^2 = x^2 \Rightarrow 2|x \Rightarrow x = 2z \wedge z \in \mathbb{Z} \Rightarrow 2y^2 = 4z^2 \Rightarrow y^2 = 2z^2 \Rightarrow 2|y \Rightarrow 2|x \wedge 2|y$$

was natürlich nicht funktioniert, da $\frac{x}{y}$ schon ein gekürzter Bruch ist.
Die Menge $\mathbb{R} \setminus \mathbb{Q}$ ist die Menge der irrationalen Zahlen. Die oben angegebene Definition der reellen Zahlen ist mathematisch nicht korrekt, da der Begriff der Kommazahl in der Mathematik nicht existiert. Die exakte Definition der reellen Zahlen ist sehr kompliziert.

[1] Ein Ergebnis aus der Mengenlehre sagt sogar das merkwürdige Resultat, dass die Menge $\mathbb{N}$ genauso groß ist wie die Menge $\mathbb{Z}$.

Man macht es mit sogenannten Dedkindschen Schnitten.
Es gilt die folgende Beziehung

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$$

Im folgenden sind noch einige spezielle Teilmengen dieser Zahlen hervorgehoben.

- $\mathbb{Z}_+ = \{x : x \in \mathbb{Z} \wedge x > 0\}$ die Menge der positiven ganzen Zahlen
- $\mathbb{Q}_+ = \{x : x \in \mathbb{Q} \wedge x > 0\}$ die Menge der positiven rationalen Zahlen
- $\mathbb{R}_+ = \{x : x \in \mathbb{R} \wedge x > 0\}$ die Menge der positiven reellen Zahlen
- $\mathbb{Z}_- = \{x : x \in \mathbb{Z} \wedge x < 0\}$ die Menge der negativen ganzen Zahlen (analog $\mathbb{Q}$ und $\mathbb{R}$)

Es sei noch bemerkt, dass die Zahl 0 weder positiv noch negativ ist.

## 1.4 Abbildungen

Abbildungen hat man oft schon unterbewusst benutzt. Beispielsweise wenn man ein Rechteck gegeben hat, so kann man deren Umfang oder deren Flächeninhalt berechnet. Die Idee einer Abbildung besteht nun darin jedem Element einer Menge $A$ ein Element einer Menge $B$ zuzuordnen. In unserem Fall ordnen wir der Menge aller Rechtecke $A$ den Umfang zu, also ein Element aus der Menge $\mathbb{R}$ zu. Man kann auch der Menge der ganzen Zahlen $\mathbb{Z}$ wieder ein Element der ganzen Zahlen $\mathbb{Z}$ zuordnen, indem man jeder Zahl ihr doppeltes zuordnet. Man kann dann so einer Abbildung auch einen Namen geben und schreibt dann $f : A \to B$. Das $f$ ist der Name der Abbildung, die Menge $A$ ist der Definitionsbereich und die Menge $B$ ist der Wertebereich. Die Abbildung $f$ ordnet jedem Element des Definitionsbereichs eindeutig ein Element des Wertebereichs zu. Die können wir noch mal als Definition schreiben.

**Definition 10** *Eine Abbildung $f : A \to B$ ist eine eindeutige Zuordnung bei der jedem Element des Definitionsbereichs $A$ ein Element des Wertebereichs $B$ zugeordnet wird.*

Sei $f : A \to B$ eine Abbildung und ein Element $a \in A$ wird dem Element $b \in B$ zugeordnet, dann schreibt man $f(a) = b$ (sprich $f$ von $a$ ist gleich $b$).

**Beispiele:**

- Es werde jeder natürlichen Zahl ihren Nachfolger zugeordnet und diese Abbildung soll $n$ heißen. Es ist dann $n : \mathbb{N} \to \mathbb{N}$ mit $n(k) = k + 1$.
- Es sei $f : \mathbb{N} \to \mathbb{N}$ eine Abbildung mit $f(n) = n^2$. Die Abbildung $f$ ordnet jeder natürlichen Zahl ihr Quadrat zu.

- Sei $f : \{1;2\} \to \{3;4;5\}$ mit $f(1) = 3, f(1) = 4, f(2) = 5$, dann ist $f$ **keine** Abbildung, da der 1 nicht eindeutig ein Element des Wertebereichs zugeordnet wird.
- $f : \mathbb{N} \to \mathbb{N}$ mit $f(k) =$ Anzahl der Teiler von $k$ ist eine Abbildung. Es ist beispielsweise $f(12) = 6$, da die 12 genau 6 Teiler hat, nämlich $1, 2, 3, 4, 6, 12$.
- $f : \mathbb{N} \to \mathbb{N}$ mit $f(k) = \sqrt{k}$ ist keine Abbildung, da z.B. $\sqrt{2} \notin \mathbb{N}$ ist.
- $f : \mathbb{N} \to \mathbb{R}_+$ mit $f(k) = \sqrt{k}$ ist eine Abbildung.
- $f : \mathbb{N} \to \mathbb{R}$ mit $f(k) = \sqrt{k}$ ist keine Abbildung, da z.B. $f(4) = 2$, aber auch $f(4) = -2$ ist.
- $f : \mathbb{N} \to \mathcal{P}(\mathbb{N})$ mit $f(k) = \{n : n \in \mathbb{N} \wedge n|k\}$ ist eine Abbildung. Es wird jeder natürlichen Zahlen die Menge ihrer Teiler zugeordnet. Beispielsweise ist $f(12) = \{1; 2; 3; 4; 6; 12\}$ oder $f(0) = \mathbb{N} \setminus \{0\}$.

In der Mathematik geht man manchmal nicht exakt mit dem Begriff der Abbildung um. Betrachtet man beispielsweise die Abbildung $f : \mathbb{R} \to \mathbb{R}$ mit $f(x) = \frac{1}{x}$, so ist dies keine Abbildung, da $f(0) = \frac{1}{0}$ nicht definiert ist. Der 0 wird also kein Element des Wertebereichs zugeordnet. Man sagt die Abbildung $f$ ist an der Stelle 0 nicht definiert. Solche Abbildungen (die eigentlich keine sind) wollen wir auch zulassen.

Wir wollen nun eine weitere wichtige Mengenoperation einführen, das Kreuzprodukt von Mengen.

**Definition 11** *Seien $A$ und $B$ Mengen, dann ist das Kreuzprodukt $A \times B$ der Mengen die Menge*

$$A \times B = \{(a, b) : a \in A \wedge b \in B\}$$

Das Kreuzprodukt $A \times B$ von zwei Mengen ist also die Menge aller Paare $(a, b)$, wobei die erste Komponente aus der Menge $A$ kommt und die zweite Komponente aus der Menge $B$ kommt. Sei beispielsweise $A = \{1, 2, 3\}$ und $B = \{2, 3, 4\}$, dann ist $A \times B = \{(1, 2); (1, 3); (1, 4); (2, 2); (2, 3); (2, 4); (3, 2); (3, 3); (3, 4)\}$. Zwei Paare (Elemente eines Kreuzprodukts von Mengen) sind genau dann gleich, wenn sie in ihren Komponenten übereinstimmen. Es ist also $(a, b) = (c, d)$ wenn $a = c$ und $b = d$. Die Paare $(1, 2)$ und $(2, 1)$ sind nicht gleich. Bei diesen Paaren kommt es auf die Ordnung an, deshalb nennt man diese Paare oft auch geordnete Paare. Mit Hilfe dieser Operation können wir auch Mengen ganz anders beschreiben. Es sei $R$ die Menge aller Rechtecke mit den Seiten $a$ und $b$. Wir wissen, dass ein Rechteck durch die Seitenlängen $a$ und $b$ eindeutig festgelegt ist, also kann man die Menge $R$ auch schreiben als $\mathbb{R}_+ \times \mathbb{R}_+$. Diese Menge besteht aus allen Paaren deren Komponenten positive reelle Zahlen sind. Wir wollen jetzt die Abbildung beschreiben die jedem Rechteck sein Flächeninhalt zuordnet. Wir nennen diese Abbildung $A$ gemäß der Bezeichnung für Flächeninhalte. Der Flächeninhalt eines Rechtecks mit den Seiten $a$ und $b$ ist gerade das Produkt $a \cdot b$. Die Abbildung lautet also

$$A : \mathbb{R}_+ \times \mathbb{R}+ \to \mathbb{R}_+ \quad (a, b) = a \cdot b$$

Es ist also $A(a,b) = a \cdot b$.
Wir können unsere Definition des Kreuzprodukt zweier Mengen auch auf mehr als zwei Mengen ausdehnen.

**Definition 12** *Seien $A_1, \ldots, A_k$ Mengen, dann ist $A_1 \times, \ldots, A_k$ die Menge*

$$A_1 \times \ldots \times A_k = \{(a_1, \ldots, a_k) : a_1 \in A_1 \wedge \ldots \wedge a_k \in A_k\}$$

Das Kreuzprodukt von $k$ Mengen ist also eine Menge aus $k$-Tupeln. Wegen der Schreibweise führen wir noch eine Definition an.

**Definition 13** *Sei $A$ eine Menge, dann schreibt man*

$$\underbrace{A \times \ldots \times A}_{k\text{-mal}} = A^k.$$

Die Menge $\mathbb{R}^3$ besteht beispielsweise aus allen Tripeln $(a,b,c)$, wobei $a, b$ und $c$ reelle Zahlen sind.

## 1.5 injektive, surjektive und bijektive Abbildungen

Wir haben im vorigen Abschnitt den Begriff der Abbildungen kennengelernt. Eine Abbildung kann viele Eigenschaften haben. Drei wichtige Eigenschaften werden wir im folgenden kennenlernen. Wir müssen dazu noch einige Begriffe einführen.

**Definition 14** *Sei $f : A \to B$ eine Abbildung, die Menge*

$$Im(f) = \{f(x) : x \in A\}$$

*heißt das Bild der Abbildung.*

Die Menge $Im(f)$ ist also die Menge aller Werte die die Abbildung $f$ annehmen kann. Das Bild einer Abbildung ist also eine Teilmenge des Wertebereichs, in Zeichen ausgedrückt heißt dies $Im(f) \subseteq B$.

**Beispiele:**

- Sei $A = \{1,2,3\}$ und $f : A \to \mathbb{Z}$ eine Abbildung mit $f(x) = x + 1$, dann ist $Im(f) = \{2,3,4\}$, denn es ist $f(1) = 2$,$f(2) = 3$ und $f(3) = 4$.
- Sei $f : \mathbb{Z} \to \mathbb{Z}$ eine Abbildung mit $f(x) = x^2$, dann ist $Im(f)$ die Menge aller Quadratzahlen.
- Sei $I = \{x \in \mathbb{R} : 0 < x < 1\} = (0,1) \subseteq \mathbb{R}$ ein offenes Intervall. Wir betrachten die Abbildung $f : I \to \mathbb{R}$ mit $f(x) = \frac{1}{x}$, dann ist $Im(f) = (1,\infty) = \{x \in \mathbb{R} : 1 < x\}$
- Wir betrachten wieder das offene Intervall $I = (0,1)$ und die Abbildung $f : I \to \mathbb{R}$ mit $f(x) = x + 2$, dann ist $Im(f) = (2,3)$.

Um weitere Definitionen vornehmen zu können führen wir wieder neue Symbole ein. Das Symbol $\forall$ heißt wörtlich "für alle". Der Ausdruck $\forall x \in \mathbb{Z}$ würde somit heißen, für alle ganzen Zahlen. Das Symbol $\exists$ bedeutet "es existiert" bzw. "es gibt". Der Ausdruck $\exists x \in \mathbb{R}$ heißt dann es existiert eine reelle Zahl.

***Bemerkung:*** *So wie wir die Symbole $\forall$ und $\exists$ eingeführt haben soll es nur dem Verständnis dienen, es ist keine mathematisch exakte Definition.*

**Beispiele:**

- Die Menge $M = \{x : \exists n \in \mathbb{Z} : x = n^2\}$ ist die Menge der Quadratzahlen. Die Menge würde sprachlich das Gleiche bedeuten wie: Alle $x$ mit der Eigenschaft, es existiert eine ganze Zahl $n$ mit $n^2 = x$.
- Die Eigenschaft, dass jede natürliche Zahl einen Nachfolger hat kann man dann auch folgendermaßen schreiben: $\forall x \in \mathbb{N} \exists y \in \mathbb{N} : y = x + 1$.

Wie oben gesagt wollen wir wichtige Eigenschaften von Abbildungen kennenlernen.

**Definition 15** *Es sei $f : A \to B$ eine Abbildung. Gilt für die Abbildung*

$$x \neq y \Rightarrow f(x) \neq f(y),$$

*so heißt die Abbildung $f$ injektiv. Eine injektive Abbildung nennt man eine Injektion.*

**Beispiele:**

- Es sei $f : M \to M$ eine Abbildung mit $f(x) = x$. Die Abbildung $f$ ist eine Injektion, sie wird die Identitätsabbildung genannt.
- $f : \mathbb{Z} \to \mathbb{Z}$ mit $f(x) = x + 1$ ist eine Injektion.
- $f : \mathbb{Z} \to \mathbb{Z}$ mit $f(x) = x^2$ ist keine Injektion, da beispielsweise $-1 \neq 1 \Rightarrow f(-1) = 1 = f(1)$.
- Sei $f : \mathbb{R} \to \mathbb{R}$ eine monotone[2] Abbildung, dann ist $f$ injektiv, da aus $x \neq y \Rightarrow x < y \wedge x > y$ und somit auch $f(x) < f(y)$ oder $f(x) > f(y)$ und somit auf jeden fall $f(x) \neq f(y)$.
- $f : \mathbb{R}^2 \to \mathbb{R}$ mit $f(x, y) = x \cdot y$ ist nicht injektiv, da beispielsweise $f(1, 2) = f(2, 1)$ ist. Wir hatten oben gesagt, dass die Paare $(1, 2)$ und $(2, 1)$ nicht gleich sind.

**Definition 16** *Es sei $f : A \to B$ eine Abbildung. Gilt für die Abbildung*

$$Im(f) = B$$

*so heißt die Abbildung $f$ surjektiv. Eine surjektive Abbildung nennt man eine Surjektion.*

[2]Eine Abbildung heißt monoton wachsend, falls $x < y \Rightarrow f(x) < f(y)$ und sie heißt monoton fallend, falls $x < y \Rightarrow f(x) > f(y)$. Eine Abbildung die entweder monoton wachsend oder monoton fallend ist heißt monoton.

Bei einer surjektiven Abbildung wird also jedes Element im Wertebereich mindestens einmal angenommen. Man hätte eine Surjektion auch anders definieren können, uns zwar: Eine Abbildung $f : A \to B$ heißt Surjektion, falls

$$\forall y \in B \exists x \in A : f(x) = y.$$

Mit anderen Worten heißt dies, dass für alle Elemente $y \in B$ gibt es ein Element $y \in A$, so dass $y = f(x)$ ist, dieses Element $y$ also wirklich als Funktionswert auftritt.

**Beispiele:**

- Die Identitätsabbildung ist surjektiv.
- $f : \mathbb{Z} \to \mathbb{Z}$ mit $f(x) = x+1$ ist surjektiv. Wir können nämlich zu jeder ganzen Zahl $y$ eine ganze Zahl $x$ finden mit $y = x + 1$.
- Die Abbildung $f : \mathbb{N} \to \mathbb{N}$ mit $f(x) = x+1$ ist nicht surjektiv, da es keine natürliche Zahl $x$ gibt mit $f(x) = 0$.
- $f : \mathbb{R} \to \mathbb{R} \setminus \{0\}$ mit $f(x) = \frac{1}{x}$ ist surjektiv.
- $f : \mathbb{R}^2 \to \mathbb{R}$ mit $f(x, y) = x + y$ ist surjektiv. Man betrachte $f(x, 0)$.
- $f : \mathbb{R} \to \mathbb{R}$ mit $f(x) = x^2$ ist nicht surjektiv, da es beispielsweise keine reelle Zahl $x$ gibt mit $f(x) = -1$.

Wie wir gesehen haben hängt die Eigenschaft einer Abbildung injektiv oder surjektiv zu sein nicht nur von der Abbildung selbst ab, sondern auch von den Definitions- und Wertebereichen ab.

**Definition 17** *Eine Abbildung $f$ heißt bijektiv, wenn sie injektiv und surjektiv ist. Eine bijektive Abbildung nennt man auch Bijektion.*

Ist die Abbildung $f : A \to B$ bijektiv, so gibt es zu jedem Element $y \in B$ genau ein $x \in A$ mit $f(x) = y$.

**Beispiele:**

- Die Identitätsabbildung ist bijektiv.
- $f : \mathbb{Z} \to \mathbb{Z}$ mit $f(x) = x + 1$ ist bijektiv.
- Jede lineare, nicht konstante Funktion $f : \mathbb{R} \to \mathbb{R}$ ist bijektiv.
- Die Abbildung $ff : \mathbb{R} \to \mathbb{R}$ mit $f(x) = x^2$ ist nicht bijektiv, da sie nicht surjektiv ist.

Diese Eigenschaften sind für Abbildungen fundamental. Besonderes interessant für die Mathematik sind bijektive Abbildung. Gibt es eine Bijektion zwischen zwei endlichen Mengen, so haben sie die gleiche Anzahl an Elementen und sind somit gleichmächtig. Man definiert deshalb zwei unendlichen Mengen als gleichmächtig, wenn eine Bijektion zwischen ihnen existiert. Mit der dieser Definition der Gleichmächtigkeit von Mengen kommt man dann zu den erstaunlichen Resultat, dass die Menge der rationalen Zahlen gleichmächtig der Menge der natürlichen Zahlen ist, als $|\mathbb{Q}| = |\mathbb{N}|$. Mit Aussagen über die Gleichmächtigkeit von mengen wollen wir uns hier nicht weiter beschäftigen. Wir definieren noch eine Operation zwischen Abbildungen.

**Definition 18** *Seien $f : A \to B$ und $g : B \to C$ Abbildungen, dann ist*

$$(g \circ f)(x) = g(f(x))$$

*die Hintereinanderausführung der Abbildungen.*

Wir betrachten beispielsweise die Abbildungen $f : \mathbb{R} \to \mathbb{R}$ mit $f(x) = ax + b$ und $g : \mathbb{R} \to \mathbb{R}$ mit $f(x) = x^2$, dann ist $(g \circ f)(x) = (ax + b)^2$.

**Satz 1** *Seien $f : A \to B$ und $g : B \to C$ injektive, surjektive oder bijektive Abbildungen, dann ist die Abbildung $g \circ f$ wieder injektiv, surjektiv oder bijektiv.*

**Beweis:**
injektiv: Seien $f$ und $g$ injektiv. Wir haben dann zu zeigen, dass für je zwei $x, y \in A$ mit $x \neq y$ folgt $(g \circ f)(x) \neq (g \circ f)(y)$. Nach Voraussetzung ist $f$ injektiv, also gilt für $x \neq y \Rightarrow f(x) \neq f(y)$. Sei $f(x) = u$ und $f(y) = v$, dann ist $u \neq v$ und da $g$ injektiv ist gilt $g(u) \neq g(v)$ und somit $g(f(x)) \neq g(f(y))$. Dies bedeutet aber gerade $(g \circ f)(x) \neq (g \circ f)(y)$.
surjektiv: Seien $f$ und $g$ surjektiv. Es ist dann $B = f(A)$ und $C = g(B) = g(f(A)) = (g \circ f)(A)$.
bijektiv:Seien $f$ und $g$ bijektiv, dann sind $f$ und $g$ injektiv und surjektiv, somit ist auch $g \circ f$ injektiv und surjektiv und somit bijektiv.

# 2 Gruppen

## 2.1 Gruppen

Bei der Untersuchung vieler Probleme gelangt man oft zu immer wiederkehrenden Strukturen. Man braucht nur die Addition von ganzen Zahlen zu betrachten. Sie ist assoziativ, sie ist kommutativ usw. . das Gleiche gilt für die Multiplikation, sie ist assoziativ und kommutativ. Wir können auch noch komplizierter werden und Polynome betrachten, das sind Abbildungen von $\mathbb{R} \to \mathbb{R}$ mit $f(x) = a_0 + a_1 x + \ldots + a_n x^n$ wobei die $a_n$ sämtlich reelle Zahlen sind. Man kann auch zwei Polynome miteinander multiplizieren und erhält wieder ein Polynom, man erhält sogar noch mehr, diese Multiplikation ist assoziativ und kommutativ. Diese Entdeckungen legen es nahe solche Mengen auf denen eine Operation definiert ist gesondert zu betrachten. Eine Menge mit Operationen nennt man eine algebraische Struktur. So ist zum Beispiel die Menge der ganzen Zahlen mit der Addition eine algebraische Struktur. Der Teilbereich der Mathematik der sich mit algebraischen Strukturen beschäftigt ist die Algebra. Wir wollen uns hier auf eine spezielle algebraische Struktur beschränken und zwar den Gruppen.

**Definition 19** *Es sei $G$ eine Menge und $\circ$ eine Operation auf der Menge $G$. Das Paar $(G, \circ)$ heißt eine Gruppe falls die folgenden Eigenschaften erfüllt sind.*

*(i)* $g_1, g_2 \in G \Rightarrow g_1 \circ g_2 \in G$

*(ii)* $g_1, g_2, g_3 \in G \Rightarrow (g_1 \circ g_2) \circ g_3 = g_1 \circ (g_2 \circ g_3)$ *(Assoziativgesetz)*

*(iii)* $\exists e \in G : g \circ e = e \circ g = g \forall g \in G$ *(Existenz des neutralen Elementes)*

*(iv)* $\forall g \in G \exists g^{-1} \in G : g \circ g^{-1} = g^{-1} \circ g = e$ *(Existenz des inversen Elementes)*

*Gilt zusätzlich das Kommutativgesetz*

$$g_1 \circ g_2 = g_2 \circ g_1 \forall g_1, g_2 \in G$$

*so heißt die Gruppe abelsch.*

Die Bedingungen $(i) - (iv)$ nennt man Gruppenaxiome. Wir wollen die Bedeutung dieser Axiome anhand eines Beispieles nachvollziehen. Wir betrachten die Menge der ganzen Zahlen $\mathbb{Z}$. Auf dieser Menge erklären wir die übliche Addition $(+)$ als Verknüpfung. Das Paar $(\mathbb{Z}, +)$ ist dann eine algebraische Struktur, da auf dieser Menge eine Verknüpfung erklärt ist. Das Paar $(\mathbb{Z}, +)$ ist sogar eine Gruppe. Das Axiom $(i)$ besagt, dass wenn man

zwei Elemente miteinander Verknüpft, so erhält man wieder ein Element aus der selben Mengen. Wir können zwei ganze Zahlen miteinander addieren und erhalten wieder eine ganze Zahl. Das Axiom $(i)$ ist also erfüllt. Das Axiom $(ii)$ ist nichts Anderes als das gewöhnliche Assoziativgesetz der ganzen Zahlen wir können die Klammern also beliebig setzen. Das Axiom $(iii)$ besagt, dass es ein neutrales Element in dieser Menge gibt. Das neutrale Element in der Gruppe $(\mathbb{Z}, +)$ ist die 0. Für die 0 gilt $a + 0 = 0 + a = a$. Das neutrale Element ist also ein Element, so dass wenn man es mit irgendein Element $g$ verknüpft, man das selbe Element $g$ wieder erhält. Das Axiom $(iv)$ besagt, dass es zu jedem Element aus der Gruppe ein inverses Element gibt. Im Fall der Gruppe $(\mathbb{Z}, +)$ wäre das inverse Element zu $a$ das Element $-a$. Es gilt nämlich $a+(-a) = (-a)+a = 0$. Verknüpft man ein Element mit seinem inversen Element, so erhält man das neutrale Element. Für die Gruppe $(\mathbb{Z}, +)$ gilt bekanntlich das Kommutativgesetz, also ist die Gruppe $(\mathbb{Z}, +)$ eine abelsche Gruppe.
Betrachten wir nun das Paar $(\mathbb{Z}, \cdot)$ mit der üblichen Multiplikation als Verknüpfung, so ist das Paar $(\mathbb{Z}, \cdot)$ keine Gruppe. Es sind zwar die Axiome $(i), (ii)$ und $(iii)$ erfüllt, aber das Axiom $(iv)$ ist nicht erfüllt. Es gibt beispielsweise zur 2 kein multiplikativ inverses Element in $\mathbb{Z}$. Das multiplikativ inverse Element zur 2 wäre $\frac{1}{2}$ und dies ist keine ganze Zahl.

**Beispiele:**

- Das Paar $(\mathbb{N}, +)$ ist keine Gruppe, da es in der Menge $\mathbb{N}$ nicht zu jedem Element ein inverses Element gibt.
- Die Paare $(\mathbb{Q}, +)$ und $(\mathbb{Q} \setminus \{0\}, \cdot)$ sind abelsche Gruppen.
- Es sei $P$ die Menge der Polynome, dann ist das Paar $(P, +)$ eine abelsche Gruppe. Das neutrale Element ist die 0 und zu einem Polynom $p(x)$ ist $-p(x)$ das inverse.
- Sei wieder $P$ die Menge aller Polynome, das Paar $(P \setminus \{0\}, \cdot)$ ist keine Gruppe. Beispielsweise existiert für das Polynom $x + 1$ kein inverses Element in $P$.

**Aufgabe:**Sei $M$ die Menge aller Zahlen der Form $a + b\sqrt{D}$, wobei $a, b, D \in \mathbb{Z}$ und $D$ keine Quadratzahl ist. Sei $+$ die übliche Addition. Man beweise, dass das Paar $(M, +)$ eine abelsche Gruppe ist. Ist auch $(M, \cdot)$, wobei $\cdot$ die übliche Multiplikation ist, eine Gruppe?

**Lösung:**
Axiom (i) Sei $a+b\sqrt{D}, c+d\sqrt{D} \in M$, dann ist $a+b\sqrt{D}+c+d\sqrt{D} = (a+c)+(b+d)\sqrt{D}$ offensichtlich auch wieder in $M$.
Axiom (ii) trivial.
Axiom (iii) Das neutrale Element ist 0.
Axiom (iv) Sei $a+b\sqrt{D} \in M$, dann ist $-a-b\sqrt{D}$ das inverse Element, denn $a+b\sqrt{D}+(-a-b\sqrt{D}) = 0$.

Das die Gruppe abelsch ist folgt aus der Kommutativität der Addition.
Das Paar $(M, \cdot)$ ist keine Gruppe. Es gibt nicht zu jedem Element ein inverses. Man betrachte $1+\sqrt{D}$, dann ist $\frac{1}{1+\sqrt{D}} = \frac{1-\sqrt{D}}{(1-\sqrt{D})(1+\sqrt{D})} = \frac{1-\sqrt{D}}{1-D} = \frac{1}{1-D} - \sqrt{D}\frac{1}{1-D}$. Es ist $D > 1$, da $D$ keine Quadratzahl ist, also ist $\frac{1}{1-D} \notin \mathbb{Z}$ und somit $\frac{1}{1-D} - \sqrt{D}\frac{1}{1-D} \notin M$. Die Zahl $1+\sqrt{D}$ besitzt also kein inverses in $M$.

**Aufgabe:** Sei $L$ die Menge der linearen und nichtkonstanten Abbildungen $\mathbb{R} \to \mathbb{R}$, also die Menge der Abbildung der Form $f(x) = ax + b$ mit $a \neq 0$. Es sei $\circ$ die Hintereinanderausführung der Abbildungen. Man beweise, das Paar $(L, \circ)$ ist eine Gruppe.

**Lösung:**
Axiom (i) Seien $f, g \in L$, also $f(x) = ax + b$ und $g(x) = cx + d$, dann ist $(f \circ g)(x) = f(g(x)) = a(cx + d) + b = acx + ad + b \in L$.
Axiom (ii) Sei $f, g, h \in L$, dann ist $f \circ (g \circ h) = f((g \circ h)(x)) = f(g(h(x))) = (f \circ g)(h(x)) = (f \circ g) \circ h$.
Axiom (iii) Das neutrale Element ist die Identitätsabbildung, also $id(x) = x$, denn $(f \circ id)(x) = (ax + b) \circ (x) = ax + b = f(x)$, analog $(id \circ f)(x) = (x) \circ (ax + b) = ax + b = f(x)$.
Axiom (iii) Sei $f(x) = ax + b$. Das inverse Element $f^{-1}(x)$ von $f(x)$ ist dann $f(x) = \frac{1}{a}x - \frac{b}{a}$. Es gilt nämlich $(f \circ f^{-1})(x) = a\left(\frac{1}{a}x - \frac{b}{a}\right) + b = x - b + b = x = id(x)$, analog $(f^{-1} \circ f)(x) = \frac{1}{a}(ax + b) - \frac{b}{a} = x + \frac{b}{a} - \frac{b}{a} = x = id(x)$.
Diese Gruppe ist nicht abelsch, da beispielsweise für $f(x) = x + 1$ und $g(x) = 2x$ gilt $(f \circ g)(x) = 2x + 1$, aber $(g \circ f)(x) = 2x + 2$.

**Aufgabe:** Sei $A$ eine Menge. Sei $B$ die Menge aller Bijektionen von $A$ nach $A$. Man beweise, dass die Menge $B$ zusammen mit der Hintereinanderausführung eine Gruppe ist.

**Lösung:**
Axiom (i) Dies folgt aus Satz 1
Axiom (ii) Seien $f, g, h \in B$, dann ist $f \circ (g \circ h) = f((g \circ h)(x)) = f(g(h(x))) = (f \circ g)(h(x)) = (f \circ g) \circ h$.
Axiom (iii) Das neutrale Element ist die Identitätsabbildung, also $id(x) = x$.
Axiom (iv) Sei $f \in B$, dann ist $f$ bijektiv. Es gibt also zu jedem Element $a \in A$ genau ein Element $a' \in A$ mit $f(a) = a'$. Wir definieren die folgende Abbildung $f^{-1}(x)$ als die Abbildung die jedem Element $a'$ das Element $a$ zuordnet, so dass $f(a) = a'$ ist. $f^{-1}$ ist dann eine Abbildung, denn es gibt zu jedem Element $a'$ genau ein $a$ mit $f(a) = a'$, da $f$ surjektiv und injektiv ist. Die Abbildung $f^{-1}$ ist die Umkehrabbildung zu $f$. Sie ist offensichtlich wieder bijektiv.

Zur Vereinfachung machen wir noch eine **Vereinbarung**. Anstatt zwischen zwei Elementen immer das Zeichen $\circ$ zu schreiben, lassen wir es wie beim Multiplikationszeichen einfach weg. Es heißt in Zukunft also $g_1 g_2$ anstatt $g_1 \circ g_2$.
Wir wollen nun noch einige Eigenschaften über die Elemente von Gruppen herausstellen. Es könnte doch sein, dass es Gruppen gibt die mehr als nur ein neutrales Element besitzen. Genauso gut könnte es zu einem Element in der Gruppe mehrere inverse Elemente geben. Das folgende Lemma sagt uns das es soetwas nicht geht.

**Lemma 1** *Sei $(G, \circ)$ eine Gruppe, dann gibt es genau ein neutrales Element in $G$, desweiteren gibt es zu jedem Element in $G$ genau ein inverses Element in $G$.*

**Beweis:** Seien $e$ und $e'$ zwei neutrale Elemente in $(G, \circ)$, dann ist

$$e = ee' = e',$$

nach Axiom $(iii)$ der Gruppenaxiome.
Sei $a \in G$ und $a_1^{-1}, a_2^{-1}$ zwei inverse Elemente zu $a$, dann ist

$$a_1^{-1} = ea_1^{-1} = (a_2^{-1}a)a_1 - 1 = a_2^{-1}(aa_1^{-1}) = a_2^{-1}e = a_2^{-1}$$

Genauso wie wir Teilmengen von Mengen betrachtet haben können wir auch Untergruppen von Gruppen betrachten.

**Definition 20** *Sei $(G, \circ)$ eine Gruppe und $H \subseteq G$. Ist das Paar $(H, \circ)$ eine Gruppe, dann nennt man das Paar $(H, \circ)$ eine Untergruppe von $(G, \circ)$ und schreibt dafür*

$$H \leq G$$

**Beispiele:**

- Die Gruppe $Z = (\mathbb{Z}, +)$ ist eine Untergruppe der Gruppe $Q = (\mathbb{Q}, +)$, also $Z \leq Q$.
- Die additive[1] Gruppe der rationalen Zahlen ist eine Untergruppe der additiven Gruppe der reellen Zahlen.
- Die Gruppe die nur aus dem neutralen Element besteht ist Untergruppe jeder Gruppe.
- Sei $G$ eine Gruppe, dann ist $G \leq G$.

## 2.2 Pellsche Gleichung

Wir wollen eine kleine Anwendung der Gruppentheorie auf eine nichtlineare Diophatische Gleichung kennenlernen. Eine Diophantische Gleichung ist eine Gleichung bei der nur die ganzzahligen Lösungen interessant ist. Die Pellsche Gleichung ist eine nichtlineare Diophantische Gleichung.

[1] additiv heißt mit der gewöhnlichen Addition

**Definition 21** *Eine Pellsche Gleichung ist eine Gleichung der Form*

$$x^2 - Dy^2 = 1,$$

*wobei $x, y, D \in \mathbb{Z}$ und $D$ keine Quadratzahl ist.*

Das Problem liegt jetzt darin alle Lösungen dieser Gleichung zu finden. In der Tat, ein Satz von Landau sagt, dass es für jedes $D > 1$, welches keine Quadratzahl ist, eine Lösung gibt. Es gibt sogar unendlich viele Lösungen. Die Frage ist nur wie findet man diese Lösungen. Wenn man die Gleichung etwas genauer untersucht findet man, dass es in der Gesamtheit aller Lösungen eine gewisse Verknüpfung gibt. Wir können z.B. schreiben

$$x^2 - Dy^2 = (x + y\sqrt{D})(x - y\sqrt{D}) = 1$$

Ist also $(x, y)$ eine Lösung der Pellschen Gleichung, so könnte man Zahlen der Form $x + y\sqrt{D}$ betrachten. Als Verknüpfung zwischen zwei solchen Zahlen nehmen wir die übliche Multiplikation. Leider ist diese Menge zusammen mit der üblichen Multiplikation im Allgemeinen keine Gruppe wie wir oben gesehen haben. Wir hatten gesehen, dass nicht jede Zahl $x + y\sqrt{D}$ ein Inverses hat. Nun sind die Lösungen $(x, y)$ der Pellschen Gleichung aber eine Teilmenge der Menge $\mathbb{Z}^2$. Vielleicht hat ja die Menge der Lösungen der Pellschen Gleichung inverse Elemente. Wir betrachten aber auch nur Teilmengen von $\mathbb{Z}^2$, d.h. es muss nicht mal das Produkt zweier solcher Zahlen wieder in der Menge liegen. Untersucht man dies genauer, so erhält man

**Satz 2** *Die Menge $P \subset \mathbb{Z}^2$ aller Lösungen der Pellschen Gleichung $x^2 - Dy^2 = 1$ bildet mit der Operation $(x_1, y_1) \otimes (x_2, y_2) = (x_1x_2 + Dy_1y_2, x_1y_2 + x_2y_1)$ eine abelsche Gruppe.*

**Beweis:** Die Idee diese Operation zu wählen stammt von dem Produkt $(x_1 + y_1\sqrt{D})(x_2 + y_2\sqrt{D}) = (x_1x_2 + Dy_1y_2) + \sqrt{D}(x_1y_2 + x_2y_1)$. Wir haben also die Zahlen der Form $x_1 + y_1\sqrt{D}$ abgebildet auf das Paar $(x_1, y_1)$. Wir wollen mit den Zahlen $x_1 + y_1\sqrt{D}$ weiter arbeiten.
Axiom (i): Sei $(x_1, y_1), (x_2, y_2) \in P$, dann ist $(x_1, y_1) \otimes (x_2, y_2) = (x_1x_2 + Dy_1y_2, x_1y_2 + x_2y_1)$. Es ist dann

$$\begin{aligned}
&(x_1x_2 + Dy_1y_2)^2 - D(x_1y_2 + x_2y_1)^2 \\
&= x_1^2x_2^2 + D^2y_1^2y_2^2 + 2Dx_1x_2y_1y_2 - Dx_1^2y_2^2 - Dx_2^2y_1^2 - 2Dx_1x_2y_1y_2 \\
&= x_1^2x_2^2 + D^2y_1^2y_2^2 - Dx_1^2y_2^2 - Dx_2^2y_1^2 \\
&= (x_1^2x_2^2 - Dx_1^2y_2^2) + (D^2y_1^2y_2^2 - Dx_2^2y_1^2) \\
&= x_1^2(x_2^2 - Dy_2^2) - Dy_1^2(x_1^2 - Dy_1^2) \\
&= x_1^2 \cdot 1 - Dy_1 \cdot 1 \\
&= 1
\end{aligned}$$

Das Produkt zweier Lösungen ist also wieder eine Lösung.
Axiom (ii): Sei $(x_1, y_1), (x_2, y_2), (x_3, y_3) \in P$, dann können wir die Paare auch auffassen

als $x_1 + y_1\sqrt{D}, x_2 + y_2\sqrt{D}, x_2 + y_2\sqrt{D}$. Für diese Zahlen ist es wie das multiplizieren in reellen Zahlen und dort gilt das Assoziativgesetz ebenso gilt das Kommutativgesetz, also ist die Operation $\otimes$ auch Kommutativ.
Axiom (iii): Wir fassen die Elemente von $P$ wieder als Zahlen der Form $x_1 + y_1\sqrt{D}$ auf. Das neutrale Element ist dann 1, also das Paar $(1, 0)$. Wer daran trotzdem zweifelt kann es nachrechnen.
Axiom (iv): Beim Auffinden der inversen Elemente wird es schwieriger. Für das inverse Element $x$ einer Zahl $x_1 + y_1\sqrt{D}$ muss dann gelten $x(x_1 + y_1\sqrt{D}) = (x_1 + y_1\sqrt{D})x = 1$, also ist $x = \frac{1}{x_1+y_1\sqrt{D}}$. Erweitern wir den Bruch mit $x_1 - y_1\sqrt{D}$ so erhalten wir $\frac{x_1-y_1\sqrt{D}}{(x_1-y_1\sqrt{D})(x_1+y_1\sqrt{D})} = \frac{x_1-y_1\sqrt{D}}{x_1^2-Dy_1^2} = x_1 - y_1\sqrt{D}$. Das inverse Element zu $(x_1, y_1)$ ist also $(x_1, -y_1)$.

Als Beispiel betrachten wir die Pellsche Gleichung

$$x^2 - 5y^2 = 1.$$

Durch probieren erhält man die Lösung $(9, 4)$. Es ist also $(9, 4) \in P$. Nach Satz 2 ist $(P, \otimes)$ eine Gruppe. Eine zweite Lösung finden wir folgendermaßen $(9, 4) \otimes (9, 4) = (161, 72)$. Man könnte also auch die Paare $(9, 4) \otimes (9, 4) \otimes (9, 4), \ldots$ bilden. Dies macht deutlich, dass es unendlich viele Lösungen gibt. Erhält man so aber auch alle Lösungen? Dazu noch folgende Definition:

**Definition 22** *Seien $(x_1, y_1), (x_2, y_2) \in P$, dann ist $(x_1, y_1) < (x_2, y_2)$ genau dann wenn $x_1 + y_1\sqrt{D} < x_2 + y_2\sqrt{D}$ ist.*

Wir können also die Elemente von $P$ miteinander vergleichen. Ist $a = (x, y)$ ein Element in $P$, so ist bekanntlich $(x, -y)$, das inverse Element. Wir können nun sagen wann ein Element in $P$ positiv und wann negativ ist. Ein Element $a = (x, y)$ in $P$ ist genau dann positiv, wenn $x > 1$ ist und negativ, wenn $x < 1$ ist. Diese Definition deckt sich auch damit, dass wenn $a = (x, y)$ positiv ist, so ist auch $x + \sqrt{D}y$ positiv. Ist $x > 0$ und $y > 0$, so ist offensichtlich, dass auch $x + \sqrt{D}y > 0$ ist. Es ist dann auch $\frac{1}{x+\sqrt{D}y}$ positiv und somit ist auch $(x, -y)$ positiv. Somit ist diese Definition von positiv und negativ gerechtfertigt. Es folgt somit auch die folgende Beziehung für $a, b, c \in P$ und $c$ positiv

$$a < b \Rightarrow ac < bc.$$

Ein kleinstes positives Element $p$ ist dann ein Element mit $p \leq q$ für alle $q \in P$ und $q$ positiv.

**Satz 3** *Sei $P$ die Lösungsmenge der Pellschen Gleichung $x^2 - Dy^2 = 1$. Sei $(x, y) \in P_+$ das kleinstes positive Element , dann erhält man alle anderen Lösungen durch*

$$(x, y)^n = \begin{cases} \underbrace{(x, y) \otimes \ldots \otimes (x, y)}_{n\text{-mal}} & \text{falls } n > 0 \\ \underbrace{(x, -y) \otimes \ldots \otimes (x, -y)}_{n\text{-mal}} & \text{falls } n < 0 \end{cases}$$

*und Bildung von $(-x, y)$ von jedem Element.*

**Beweis:** Sei $(x, y) \in P$, dann ist auch $(|x|, y) \in P$. Wir brauchen also nur die Menge $\{(|x|, y) : (x, y) \in P)$ betrachten. Sei $a = (x_a, y_a) \in P_+$ das kleinste Element mit $a > (1, 0)$. Angenommen es gibt ein Element $b = (x_b, y_b) \in P$, so dass es kein $n$ gibt mit $b = a^n$. Es gibt dann eine Zahl $k$ mit $a^k < b < a^{k+1}$. Multiplizieren wir diese Gleichung mit $a^{-k}$ so erhalten wir $(1, 0) < a^{-k}b < a$, somit ist $a^{-k}b$ kleiner als $a$ und größer als $(1, 0)$ was unsere Voraussetzung widerspricht, dass $a$ das kleinste Element ist mit dieser Eigenschaft ist, also gibt kein solches Element $b$.

**Aufgabe:** Gegeben sei die Pellsche Gleichung

$$x^2 - 7y^2 = 1$$

Man finde alle ganzzahligen Lösungen dieser Gleichung.

**Lösung:** Durch probieren erhält man die Lösung $(8, 3)$ als kleinste positive Lösung. Alle anderen Lösungen haben dann die Form $(x, y) = (8, 3)^n$ oder $(x, y) = (-8, 3)^n$.
Dies ist eine Lösung mit der man zufrieden sein könnte, nur lässt sich z.B. $(8, 3)^{10}$ ohne einen Computer nicht so leicht berechnen. Wie könnte man die Lösung also bequemer angeben? Wir wissen, dass wir das Paar $(x, y)$ auch schreiben können als $x + y\sqrt{D}$. Wir wissen, dass $(x + y\sqrt{D})^n$ sich auch wieder in der Form $u + v\sqrt{D}$ darstellen lässt. Mit Hilfe der binomischen Formel erhält man dann alle Lösungen in der Form

$$x = \pm\frac{(8 + 3\sqrt{7})^n + (8 - 3\sqrt{7})^n}{2} \quad y = \frac{(8 + 3\sqrt{7})^n - (8 - 3\sqrt{7})^n}{2\sqrt{7}}$$

**Aufgabe:** Gegeben sei die Pellsche Gleichung

$$x^2 - 3y^2 = 1$$

Man finde alle ganzzahligen Lösungen dieser Gleichung.

**Lösung:**

$$x = \pm\frac{(2 + \sqrt{3})^n + (2 - \sqrt{3})^n}{2} \quad y = \frac{(8 + \sqrt{3})^n - (8 - \sqrt{3})^n}{2\sqrt{3}}$$

## 2.3 Normalteiler und der Faktorraum

Sei $G$ eine Gruppe und $U$ eine Untergruppe von $G$. Sei $g \in G$, dann können wir die Mengen $gU$ und $Ug$ bilden. Was diese Mengen bedeuten, schreiben wir noch einmal in Mengenschreibweise.

$$gU = \{gu : g \in G\} \qquad Ug = \{ug : g \in G\}$$

Die Menge $gU$ entsteht also wenn wir jedes Element in $U$ von links mit $g$ multiplizieren. Analog erhalten wir $Ug$ indem wir jedes Element von $U$ von rechts mit $g$ multiplizieren. Wir betrachten als Beispiel die Gruppe $G = (\mathbb{Z}, +)$. Sei $2\mathbb{Z}$[2] die additive Gruppe der geraden ganzen Zahlen. Man überzeugt sich leicht, dass $2\mathbb{Z}$ wieder eine Gruppe ist. Addiert man zwei gerade ganze Zahlen, so erhält man wieder eine ganze Zahl. Die Assoziativität folgt aus dem Assoziativgesetz der ganzen Zahlen. Das neutrale Element ist die 0, also gerade und das additiv inverse einer geraden ganzen Zahl ist wieder gerade. Es ist also $(2\mathbb{Z}, +) \leq (\mathbb{Z}, +)$. Sei $n \in \mathbb{Z}$ und $k \in 2\mathbb{Z}$, dann ist im Allgemeinen $k + n \notin 2\mathbb{Z}$. Ist $n$ ungerade, so ist $n + 2\mathbb{Z}$ die Menge der ungeraden Zahlen und ist $n$ gerade, so ist $n + 2\mathbb{Z} = 2\mathbb{Z}$. Betrachten wir noch ein Beispiel. Die Menge $\mathbb{R}^2$ ist die Menge aller Zahlenpaare deren Komponenten reelle Zahlen sind. Wir führen auf $\mathbb{R}^2$ eine Addition ein indem wir Komponentenweise addieren, also $(a, b) + (c, d) = (a + c, b + d)$. Wir betrachten nun die Teilmenge $D = (x, x)$, dann ist die Menge $D$ zusammen mit der komponentenweisen Addition eine abelsche Gruppe. Würde man die Menge $D$ in einem Koordinatensystem einzeichnen, so erhält man die Winkelhalbierende der Achsen vom ersten und dritten Quadranten. Die Menge $D$ ist also eine Gerade. Würde man nun ein $(a, b) \in \mathbb{R}^2$ wählen, so ist die Menge $(a, b) + D$ eine Gerade durch den Punkt $(a, b)$ und parallel zu $D$. Da die Gruppe abelsch ist , ist $(a, b) + D = D + (a, b)$.
Die Mengen die entstehen, wenn man eine Untergruppe einer Gruppe $G$ mit einem Element aus der Gruppe multipliziert nennt man Nebenklassen.

**Definition 23** *Sei $G$ eine Gruppe und $G \leq U$, dann nennt man die Mengen $gU$ die Linksnebenklassen und die Mengen $Ug$ die Rechtsnebenklassen.*

Sei $G$ eine Gruppe und $U \leq G$ eine Untergruppe, dann ist offensichtlich $e \in U$, da $e$ eindeutig ist. Somit ist $G = \bigcup_{g \in G} gU = \bigcup_{g \in G} Ug$.

**Satz 4** *Sei $G$ eine Gruppe und $U \leq G$, dann ist entweder $g_1U \cap g_2U = \varnothing$ oder $g_1U = g_2U$.*

**Beweis:** Sei $u \in U$.Angenommen es sei $g_1u \in g_2U$, dann existiert ein $v \in U$ mit $g_1u = g_2v$. Wir haben jetzt zu zeigen, dass dann für alle $w \in U$ gilt $g_1w \in U$. Es ist $g_1u = g_2v$. Multiplizieren wir diese Gleichung von rechts mit $u^{-1}$, so erhalten wir $g_1e = g_1 = g_2vu^{-1}$. Sei nun $w \in U$ beliebig. Multiplizieren wir die Gleichung von rechts mit $w$ so erhalten wir $g_1w = g_2(vu^{-1}w)$. Es ist $vu^{-1}w \in U$, da $v, u^{-1}, w \in U$ und weil $U$ eine Gruppe ist. Somit gilt für alle $w \in U$ auch $g_1w = g_2(vu^{-1}w) \in g_2U$. Also ist $g_1U \subseteq g_2U$. Analog zeigt man $g_2U \subseteq g_1U$ und somit ist $g_1U = g_2U$. Wir haben aus der Annahme, dass es nur ein Element in $g_1U \cap g_2U$ gibt geschlossen, dass dann die Mengen gleich sind. Es können also nur die oben genannten Fälle eintreten.

Wir können also sagen, dass die Nebenklassen die Menge $G$ zerlegt, also $G = \bigcup_{g \in G} gU$, wobei $g_iU \cap g_jU = \varnothing$ für $i \neq j$. Die Schreibweise $G = \bigcup_{g \in G} gU$ bedeutet, dass über alle Elemente $g$ die in $G$ liegen vereinigt wird. Die Frage ist nun, wann $gU = Ug$ ist. Haben wir es mit einer abelschen Gruppe zu tun, so gilt dies immer.

[2] Das erinnert an die eben definierte Menge $gU$

**Definition 24** *Sei $G$ eine Gruppe. Ist $U \leq G$ eine Untergruppe von $G$ und gilt $gU = Ug$ für alle $g \in G$, so nennt man die Untergruppe einen Normalteiler und schreibt dafür $U \trianglelefteq G$.*

Betrachten wir weiterhin die Menge aller Nebenklassen von $U \leq G$. Ist sogar $U \trianglelefteq G$, so sind die Rechts- und die Linksnebenklassen identisch. Wir definieren auf der Menge aller Nebenklassen eine Operation mit $g_1U \otimes g_2U = g_1g_2U$. Wir multiplizieren also Mengen miteinander. Bei dieser Operation tritt nun ein Problem auf, die Wohldefiniertheit. Wir hatten oben die Gruppe $G = (\mathbb{Z}, +)$ betrachtet. Wir hatten gesehen, dass die Gruppe $N = (2\mathbb{Z}, +)$ eine Untergruppe von $G$ ist und da $G$ sogar abelsch ist, ist $N \trianglelefteq G$. Die einzige Nebenklasse von $N$ war die Menge der ungeraden Zahlen und die können wir auf mehrere Arten darstellen und zwar einmal mit $1+2\mathbb{Z}$ aber auch als $3+2\mathbb{Z}$. Es taucht nun die Frage auf, wenn $g_1U = g_1'U$ ist, ist dann auch $g_1U \otimes g_2U = g_1'U \otimes g_2U$? Die Frage können wir positiv beantworten. Es ist $(g_1g_2)U = g_1U \otimes g_2U = g_1'U \otimes g_2U = (g_1'g_2)U$, also stimmen beide Produkte überein.

**Satz 5** *Sei $G$ eine Gruppe und $N \trianglelefteq G$ ein Normalteiler, dann ist die Menge $\{gN : g \in G\}$ zusammen mit der Operation $\otimes$ eine Gruppe.*

**Beweis:**
Axiom (i): Sind $g_1N$ und $g_2N$ zwei Nebenklassen von $N$, so ist $g_1N \otimes g_2N = g_1g_2N$ wieder eine Nebenklasse, da $g_1g_2 \in G$ ist.
Axiom (ii): Die Assoziativität folgt aus der Assoziativität der Gruppe.
Axiom (iii): Das neutrale Element ist $N$, denn $gN \otimes N = gN \otimes eN = (ge)N = gN$.
Axiom (iv): Sei $gN$ eine Nebenklasse, dann ist $g^{-1}N$ das inverse zu $gN$, denn $gN \otimes g^{-1}N = (gg^{-1})N = eN = n$ und analog $g^{-1}NgN = N$.

**Definition 25** *Sei $G$ eine Gruppe und $N \trianglelefteq G$ ein Normalteiler. Die Gruppe $(\{gN : g \in G\}, \otimes)$ heißt die Faktorgruppe und wird mit*

$$G/N$$

*bezeichnet. [sprich $G$ modulo $N$.]*

## 2.4 Die additive Gruppe $\mathbb{Z}/n\mathbb{Z}$

Wir hatten im vorigen Abschnitt die Nebenklassen von $2\mathbb{Z}$ als Untergruppe der Gruppe $(\mathbb{Z}, +)$ betrachtet. Dies wollen wir verallgemeinern. Sei $n$ eine positive ganze Zahl, dann ist die Menge $n\mathbb{Z}$[3] zusammen mit der gewöhnlichen Addition eine Gruppe. $n\mathbb{Z}$ ist also eine Untergruppe von $(\mathbb{Z}, +)$ und da die Gruppe $(\mathbb{Z}, +)$ abelsch ist, ist $n\mathbb{Z}$ sogar ein Normalteiler. Wir können also die Faktorgruppe $\mathbb{Z}/n\mathbb{Z}$ bilden. Dies ist die additive Gruppe der Restklassen.

[3] Das ist die Menge aller durch $n$ teilbaren Zahlen.

**Definition 26** *Der Faktorraum $\mathbb{Z}/n\mathbb{Z}$ heißt die additive Gruppe der Restklassen.*

Schauen wir uns speziell die Gruppe $\mathbb{Z}/5\mathbb{Z}$ an. Das neutrale Element ist die Menge aller durch 5 teilbaren Zahlen. Bilden wir Nebenklasse $1 + 5\mathbb{Z}$ so besteht diese aus den Nachfolgern aller durch 5 teilbaren Zahlen, also alle Zahlen der Form $5k + 1$, wobei $k$ eine ganze Zahl ist. Es ist offensichtlich $6 + 5\mathbb{Z} = 1 + 5\mathbb{Z}$. Wie kann man nun entscheiden, welche Zahl in welcher Nebenklasse ist? Wir nehmen mal die Zahl 67. Die 67 ist nicht durch 5 teilbar, also $67 \notin 5\mathbb{Z}$. Es ist $67 = 2 + 65$. Die 65 ist durch 5 teilbar, also $65 \in 5\mathbb{Z}$ und somit ist $67 \in 2 + 5\mathbb{Z}$. Genauso ist die 22 in der selben Nebenklasse wie die 65, da $22 = 2 + 20$ ist und 20 durch 5 teilbar.

**Definition 27** *Wir betrachten den Faktorraum $\mathbb{Z}/n\mathbb{Z}$. Sind $a, b \in \mathbb{Z}$ in der selben Nebenklasse, so schreibt man dafür.*

$$a \equiv b \bmod n$$

*[sprich a kongruent b modulo n.]*

- Es ist $22 \equiv 67 \bmod 5$, wie oben gesehen.
- $17 \equiv 77 \bmod 10$, da $17 = 7 + 10$, $77 = 7 + 70$ und $10|10$ bzw. $10|70$.
- $15 \equiv 23 \bmod 2$, da $15 = 1 + 14$ und $23 = 1 + 22$.
- $21 \not\equiv 31 \bmod 7$, da $21 = 0 + 21$ und $31 = 3 + 28$.

**Aufgabe:** Man untersuche, welche der folgenden Aussagen wahr sind.
$12 \equiv 24 \bmod 2$; $101 \equiv 1 \bmod 10$; $13 \equiv 113 \bmod 17$
$25 \equiv 100 \bmod 5$; $19 \equiv 23 \bmod 7$; $111111 \equiv 555 \bmod 3$

Wir wissen, dass die Menge $\mathbb{Z}/n\mathbb{Z}$ zusammen mit der oben definierten Operation eine Gruppe ist. Es gilt also

$$a \equiv b \bmod n \wedge c \equiv d \bmod n \Rightarrow a + c \equiv b + d \bmod n$$

Da $a \equiv b \bmod n$ ist $a + n\mathbb{Z} = b + n\mathbb{Z}$ genauso ist $c + n\mathbb{Z} = d + n\mathbb{Z}$ und somit ist $a + c + n\mathbb{Z} = b + d + n\mathbb{Z}$.

Wir haben nun eine Operation auf der Menge $\mathbb{Z}/n\mathbb{Z}$ kennengelernt, die ähnlich der üblichen Addition ist. Wie sieht es aber mit der Multiplikation aus? Die Multiplikation wurde eingeführt um Ausdrücke wie $3 + 3 + 3 + 3 + 3 + 3 + 3 + 3$ zusammen zu fassen. Genauso wollen wir die Multiplikation auf der Menge $\mathbb{Z}/n\mathbb{Z}$ definieren.

**Definition 28** *Sei $k + n\mathbb{Z}$ ein Element von $\mathbb{Z}/n\mathbb{Z}$ und $m$ eine ganze Zahl, dann ist*

$$m \cdot (k + n\mathbb{Z}) = (k + n\mathbb{Z}) \cdot m = \underbrace{(k + n\mathbb{Z}) + \ldots + (k + n\mathbb{Z})}_{m\text{-mal}} = mk + n\mathbb{Z}$$

Wir haben also definiert was die Multiplikation einer ganzen Zahl mit einem Element aus $\mathbb{Z}/n\mathbb{Z}$ ist. Was passiert wenn wir die Zahl $m$ durch eine andere ganze Zahl ersetzen die in der selben Menge (Nebenklasse) liegt? Wir nehmen beispielsweise die Gruppe $\mathbb{Z}/7\mathbb{Z}$. Ein typisches Element aus dieser Gruppe ist $3+7\mathbb{Z}$. Es ist dann $2(3+7\mathbb{Z}) = 6+7\mathbb{Z}$. Es ist aber auch $2 \equiv 9 \bmod 7$. Ist dann auch $9(3+7\mathbb{Z}) = 2(3+7\mathbb{Z})$? Es ist $9(3+7\mathbb{Z}) = 27+7\mathbb{Z}$ und da $27 \equiv 6 \bmod 7$ ist, so ist $9(3+7\mathbb{Z}) = 2(3+7\mathbb{Z}) = 6+7\mathbb{Z}$. Die Frage ist nun gilt dies auch allgemein für alle Zahlen? Wir haben auch da wieder Glück, denn der folgende Satz sagt genau dies aus.

**Satz 6** *Seien $a, b, c, d \in \mathbb{Z}$ mit $a \equiv b \bmod n$ und $c \equiv d \bmod n$, dann gilt*

$$a + c \equiv b + d \bmod n; \qquad ac \equiv bd \bmod n$$

**Beweis:** Der Beweis für den ersten Teil ist weiter oben schon gegeben worden. Wir wollen uns also um die Multiplikation kümmern. Es ist $a \equiv b \bmod n$, also ist $a+n\mathbb{Z} = b+n\mathbb{Z}$ und somit ist gibt es ganze Zahlen $k, l$ mit $a + kn = b + nl$. Analog gibt es ganze Zahlen $p, q$ mit $c + pn = d + qn$. Es ist dann $(a + kn)(c + pn) = (b + nl)(d + qn)$ dies ist aber $ac + (ap + kc)n = bd + (bq + ld)n$. Man sieht, dass jeweils der zweite Summand durch $n$ teilbar ist, also ist $ac + n\mathbb{Z} = bd + n\mathbb{Z}$ und somit ist $ac \equiv bd \bmod n$.

Nun könnte man auch annehmen, dass die Menge $\mathbb{Z}/n\mathbb{Z}$ zusammen mit der oben definierten Multiplikation eine Gruppe bildet. Dies ist aber im Allgemeinen nicht der Fall. Der Leser möge selbst überprüfen woran es scheitert. Die Menge $\mathbb{Z}/n\mathbb{Z} \setminus \mathbb{Z}$ bildet genau bezüglich der oben definierten Multiplikation eine Gruppe, wenn $n$ eine Primzahl ist. Wir wollen noch eine **Vereinbarung** treffen. Jedesmal, wenn wir von der Menge $k + n\mathbb{Z}$ sprechen, wollen wir nicht jedesmal $k + n\mathbb{Z}$ schreiben, sondern schreiben nur einen Repräsentanten und zwar die kleinste nichtnegative ganze Zahl die in der Menge enthalten ist. Für die Menge $13 + 8\mathbb{Z}$ schreiben wir später also kurz 5 oder für die Menge $31 + 11\mathbb{Z}$ schreiben wir kurz 9. Diese Schreibweise kommt von der Division mit Rest. Es ist beispielsweise $19 : 5 = 3$ Rest 4. Die Zahl 19 liegt dann in der Menge $4 + 5\mathbb{Z}$. Es kommt also auf den Rest der Zahl $k$, bei Division durch $n$ an in welcher Menge von $\mathbb{Z}/n\mathbb{Z}$ die Zahl $k$ liegt. Man nennt die Zahlen, dann auch $n$-er Rest.

**Aufgabe:** Man beweise, dass die Summe von fünf aufeinanderfolgenden ganzen Zahlen stets durch 5 teilbar ist.

**Lösung:** Sei $n$ eine ganze Zahl, dann ist zu zeigen, dass $5|n + (n + 1) + (n + 2) + (n + 3) + (n+4)$ gilt. Einer dieser fünf Zahlen ist auf jeden Fall durch 5 teilbar. Wir nehmen an dies sei $n$. Es ist dann $n \equiv 0 \bmod 5$ und somit ist $n+(n+1)+(n+2)+(n+3)+(n+4) \equiv 0 + 1 + 2 + 3 + 4 \equiv 10 \equiv 0 \bmod 5$. Die Summe ist also in der selben Nebenklasse wie die 5. Somit ist die Aussage bewiesen.

**Aufgabe:**Man beweise, dass die Zahl

$$n = 1 + 2 + 3 + \ldots + 1000$$

durch 7 teilbar ist.

**Lösung:** Wir betrachten die Gruppe $(\mathbb{Z}/7\mathbb{Z}, +)$. Es ist $n = 1 + 2 + 3 + \ldots + 1000 = 0+1+2+3+\ldots+1000$. Nach Satz 6 ist $n \equiv 0+1+2+3+4+5+6+0+1+2+\ldots \mod 7$. Es ist $0+1+2+3+4+5+6 = 21 \equiv 0 \mod 7$. Es ist also $n = 0+0+0+\ldots \equiv 0 \mod 7$. Es ist $1000 \equiv 6 \mod 7$ und somit ist

$$n = 0+1+2+3+\ldots+1000 \equiv \underbrace{(0+1+2+3+4+5+6)+\ldots+(0+1+2+3+4+5+6)}_{\text{143-mal}} \equiv 0+\ldots+$$

Somit ist die Zahl $n$ durch 7 teilbar.
*Es ist* $n = 1 + 2 + 3 + \ldots + 1000 = 500500$.

**Aufgabe:** Man bestimme alle ganzzahligen Lösungen $(x, y)$ von

$$13x^2 - 11y^2 = 15.$$

**Lösung:** Wir betrachten die Gruppe $(\mathbb{Z}/4\mathbb{Z}, +)$. Es können nur die vier Fälle auftreten, dass $x \equiv 0 \mod 4$,$x \equiv 1 \mod 4$,$x \equiv 2 \mod 4$ oder $x \equiv 3 \mod 4$. Es folgt also, dass $x^2$ nur kongruent 0 oder 1 modulo 4 sein kann. Es ist außerdem $13 \equiv 1 \mod 4$ und $11 \equiv 3 \mod 4$ somit ist $13x^2 - 11y^2 \equiv x^2 - 3y^2 \mod 4$.
Fall 1: $x^2 \equiv 0 \mod 4$ und $y^2 \equiv 0 \mod 4$.
Dann ist $x^2 - 3y^2 \equiv 0^2 - 3 \cdot 0^2 \equiv 0 \mod 4$.
Fall 2: $x^2 \equiv 0 \mod 4$ und $y^2 \equiv 1 \mod 4$.
Dann ist $x^2 - 3y^2 \equiv 0^2 - 3 \cdot 1^2 \equiv 1 \mod 4$.
Fall 3: $x^2 \equiv 1 \mod 4$ und $y^2 \equiv 0 \mod 4$.
Dann ist $x^2 - 3y^2 \equiv 1^2 - 3 \cdot 0^2 \equiv 1 \mod 4$.
Fall 4: $x^2 \equiv 1 \mod 4$ und $y^2 \equiv 1 \mod 4$.
Dann ist $x^2 - 3y^2 \equiv 1^2 - 3 \cdot 1^2 \equiv 2 \mod 4$.
Es kann also nur $13x^2 - 11y^2 \equiv 0 \mod 4$,$13x^2 - 11y^2 \equiv 1 \mod 4$ oder $13x^2 - 11y^2 \equiv 2 \mod 4$ sein. Nun ist aber $15 \equiv 3 \mod 4$ und somit hat diese Gleichung keine Lösung.

**Aufgabe:** Man bestimme die letzte Ziffer der Zahl $7^{7^7}$.

**Lösung:** Haben wir eine ganze Zahl $n$ gegeben, so kann man sie in der Form $n = 10k+l$ schreiben, wobei $k, l \in \mathbb{Z}$ und $0 \leq l \leq 9$ ist. Die Zahl $l$ ist identisch mit der letzten

Ziffer von $n$. Wir betrachten die Gruppe $(\mathbb{Z}/10\mathbb{Z}, +)$. Bestimmen wir einmal die Nebenklassen von den Potenzen von 7. Es ist $7^0 \equiv 1 \bmod 10$, weiterhin ist $7^1 \equiv 7 \bmod 10$ und $7^2 = 49 \equiv 9 \bmod 10$. Um die Nebenklassen von höheren Potenzen zu bestimmen nutzen wir wieder Satz 6. Es ist dann $7^3 = 7^2 \cdot 7 \equiv 9 \cdot 7 \equiv 3 \bmod 10$ und $7^4 = 7^3 \cdot 7 = 3 \cdot 7 \equiv 1 \bmod 10$. Würden wir weiter machen, so wiederholen sich die Zahlen immer wieder, es würde also für die Potenzen von 7 der Reihe nach die 10-er Reste $1, 7, 9, 3, 1, 7, 9, 3, 1, \ldots$ ergeben. Man sieht, wenn die Potenz durch 4 teilbar ist, so hat die Zahl den 10-er Rest 1. Hat die Potenz den 4-er Rest 1, so hat die Zahl den 10-er Rest 7 usw. Wir haben also den 4-er Rest von $7^7$ zu bestimmen. Es ist $7^0 \equiv 1 \bmod 4$,$7^1 \equiv 3 \bmod 4$ und $7^2 = 7 \cdot 7 \equiv 3 \cdot 3 \equiv 1 \bmod 4$. Die Zahl $7^k$ lässt bei Division durch 4 den Rest 1, wenn $k$ gerade ist und 3 wenn $k$ ungerade ist. Die Zahl $7^7$ lässt also bei Division durch 4 den Rest 3 und somit lässt die Zahl $7^{7^7}$ den Rest 3 bei Division durch 10. Die letzte Ziffer der Zahl $7^{7^7}$ ist also eine 3.

**Aufgabe:** Man bestimme alle ganzzahligen Lösungen $(x, y)$ der Gleichung

$$x^2 + 2 = 13^y.$$

**Lösung:** Wir wissen aus der obigen Aufgabe, dass eine Quadratzahl bei Division durch 4 nur den Rest 0 oder 1 lässt. Die Zahl $x^2+2$ kann bei Division durch 4 somit nur die Reste 2 und 3 lassen. Betrachten wir nun die 4-er Reste der Zahlen $13^y$ für $y = 0, 1, 2, 3, 4, 5, \ldots$. Es ist $13^0 \equiv 1 \bmod 4$ und $13^1 \equiv 1 \bmod 4$. Somit lassen alle weiteren Potenzen den Rest 1 bei Division durch 4. Es muss also $x^2 + 2 \equiv 1 \bmod 4$, was nicht möglich ist wie wir oben gesehen hatten. Es existiert also keine ganzzahlige Lösung zu der Gleichung.

**Aufgabe:** Man bestimme alle ganzzahligen Lösungen $(x, y, z)$ der Gleichung

$$x^3 + y^3 = 14z^z + 3.$$

**Lösung:** Wir betrachten die Gruppe $(\mathbb{Z}/7\mathbb{Z}, +)$, also die 7-er Reste. Durch probieren erhält man, dass die Zahl $x^3$ nur die Reste $0, 1, 6$ bei Division durch 7 lässt. Die Zahl $x^3+y^3$ kann bei Division durch 7 also nur die Reste $0, 1, 2, 5, 6$ lassen. Es ist $14 \equiv 0 \bmod 7$ und somit ist $14z^z + 3 \equiv 0 \cdot z^z + 3 \equiv 3 \bmod 7$. Da auf der linken und auf der rechten Seite der Gleichung unterschiedliche Reste bei Division durch 7 auftreten existiert keine Lösung dieser Gleichung.