Vorkurs Mathematik 2010

Fabian Meier, Büro: V3-235,
eMail: vorkurs@matheistcool.de

29. September 2010

Inhaltsverzeichnis

1 Ziele des Vorkurses

Dieser Vorkurs dient dazu, den Übergang von der Schulmathematik zu der Hochschulmathematik zu erleichtern. Dabei wird es weniger darum gehen, fehlendes Wissen aufzuholen oder den Stoff des Mathe-LKs nachzuarbeiten, sondern darum, einen Zugang zu der Denk- und Arbeitsweise eines Mathematik-Studiums zu finden.

Sie werden in den folgenden zwei Wochen neun Vorlesungen hören und nachmittags jeweils Übungen dazu besuchen. Vorlesungen und Übungen werden in den nächsten zwei Semestern die beiden Veranstaltungsformen sein, mit denen Sie in Berührung kommen werden.

1.a Was ist eine Vorlesung?

Eine Vorlesung vermittelt Inhalte in komprimierter Form. Etwa 90 Minuten lang erklärt ein Dozent an der Tafel Definitionen, Sätze und Beweise, während die Studenten mitschreiben. Kurze Zwischenfragen können gestellt werden, eine Diskussion kommt aber normalerweise nicht zustande.

Aufgabe des Studenten ist es, eine ordentliche Mitschrift zu erstellen und so viel wie möglich während der Vorlesung nachzuvollziehen. Normalerweise sind 90% der Hörer einer Vorlesung damit überfordert, alle Details der Vorlesung (schon während diese stattfindet) zu verstehen. Daher besteht ein großer Teil des Mathematikstudiums aus *Nacharbeiten der Vorlesungen*. Besonders effektiv ist dies, wenn es in Gruppen stattfindet; einführende Bücher können dabei auch hilfreich sein.

Zu den Anfängervorlesungen gibt es normalerweise eine *Übung* und eine *Präsenzübung*.

1.b Was ist eine Übung?

Übungen dienen zur Besprechung der Übungsaufgaben und von Fragen zur Vorlesung. Sie finden in wesentlich kleineren Gruppen statt als Vorlesungen; in der Regel weniger als 20 Personen. Betreut werden sie meistens von einem Master- oder Promotionsstudenten (auch ältere Bachelorstudenten kommen dafür in Frage), also jemandem, der ausreichend mathematische Erfahrung mitbringt, aber auch nah an den Bedürfnissen der Studenten ist.

Es gibt zwei Arten von Übungen: Die klassischen Übungen besprechen Aufgaben, die man zu Hause bearbeitet hat. In der Regel hat man im Studium dafür eine Woche Zeit. In den Präsenzübungen, die es bei den Anfängerveranstaltungen (und im Vorkurs) gibt, löst man Übungsaufgaben in Gruppen, wobei man von einem Tutor angeleitet wird.

2 Ablaufplan

Der Vorkurs wird wie folgt ablaufen ($x \in \{239, 246, 252, 253\}$):

Tag	Zeit	Ort	Veranstaltungstyp	Bemerkungen
Mo	9-11	H15	Vorlesung	
Mo	11-13	C01-x	Übung	1. Präsenzblatt
Di	9-11	H15	Vorlesung	
Di	11-13	C01-x	Übung	2. Präsenzblatt
Mi	9-11	H15	Vorlesung	
Mi	11-13	C01-x	Übung	3. Präsenzblatt
Do	9-11	H15	Vorlesung	
Do	11-13	C01-x	Übung	4. Präsenzblatt
Fr	9-11	H15	Vorlesung	Verteilung des Heimübungsblattes
Fr	11-13	C01-x	Übung	Zeit für Fragen etc.
Mo	9-11	H15	Vorlesung	Abgabe des Heimübungsblattes
Mo	11-13	C01-x	Übung	5. Präsenzblatt
Di	9-11	H15	Vorlesung	
Di	11-13	C01-x	Übung	Heimübungsblatt
Mi	9-11	H15	Vorlesung	
Mi	11-13	C01-x	Übung	6. Präsenzblatt
Do	9-11	H15	Vorlesung	
Do	11-13	C01-x	Übung	7. Präsenzblatt
Fr	9-11	H15	Vorlesung	
Fr	11-13	C01-x	Übung	Zeit für Fragen etc.

Es finden immer fünf Übungen parallel statt, von denen man eine (jedes mal die gleiche) Übung besucht. Die Tutoren sind:

- Felix Bergunde (Tutorium in Raum C01-239)
- Henning Niesdroy (Tutorium in Raum C01-246)
- Fabian Sander (Tutorium in Raum C01-252)
- Katharina von der Lühe (Tutorium in Raum C01-253)
- Nils Ellerbrock (Tutorium in Raum C01-230)

3 Wie betreiben Mathematiker Mathematik?

Universitätsmathematik gliedert sich in drei Grundkonzepte: *Definition*, *Satz* und *Beweis*.

3.a Definitionen

Eine *Definition* legt mathematische Begriffe, wie z.B. natürliche Zahlen, lineare Funktion etc., fest. Sie darf sich dabei nur auf grundlegende mathematische Konzepte oder auf andere Definitionen stützen. Nicht erlaubt sind hingegen anschauliche Beschreibungen, unpräzise Begriffe oder außermathematische Konzepte.

Bei den folgenden Beispielen gehe ich davon aus, daß wir wissen, was eine *Menge* ist und außerdem ganze, natürliche (also positive ganze) und rationale Zahlen definiert haben (siehe auch Abschnitt 7).

Definition 3(1). Eine natürliche Zahl n heißt *gerade*, falls es eine natürliche Zahl q gibt mit $n = 2q$.

Definition 3(2). Eine rationale Zahl r heißt *invertierbar*, falls es eine rationale Zahl q gibt mit $r \cdot q = 1$.

Definition 3(3) (*falsch*)**.** Eine Funktion von $\mathbb{R}$ nach $\mathbb{R}$ heißt stetig, wenn man sie mit einem Stift in einem Zug durchzeichnen kann.

Mal abgesehen davon, daß wir $\mathbb{R}$ bisher nicht definiert haben (dies wird in Analysis 1 geschehen), sind „Stift" und „zeichnen" keine mathematischen Begriffe.

Definition 3(4) (*falsch*)**.** Eine natürliche Zahl heißt gerade, wenn sie eine der Zahlen $2, 4, 6, \ldots$ ist.

Zu unpräzise.

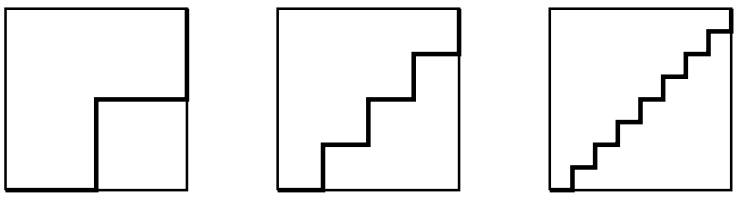
Definition 3(5). Eine natürliche Zahl n heißt *durch eine natürliche Zahl k teilbar*, wenn es eine natürliche Zahl q gibt mit $n = q \cdot k$.

Definition 3(6). Eine natürliche Zahl heißt *groß*, falls sie größer ist als jede andere natürliche Zahl.

Die letzte Definition ist korrekt, wird aber von keiner Zahl erfüllt.

Definition 3(7) (*falsch*)**.** Sei $f : \mathbb{R} \to \mathbb{R}$ eine Funktion. Dann ist ihre Ableitung $f'(x)$ bei x der Grenzwert der Sekantensteigungen, wenn man die Sekanten durch $(x, f(x))$ und $(x+h, f(x+h))$ für h gegen Null betrachtet.

Erst einmal ist „Grenzwert" ein problematischer Begriff, weil er intuitiv verstanden viele Fallen bereithält:



Die oben sichtbare Kurve „konvergiert" gegen die Diagonale, ihre Länge bleibt jedoch immer 2!

Der *Grenzwert* wird daher einer der zentralen Begriffe am Anfang von Analysis I sein.

Vorsicht ist aber noch bei einer andere Sache geboten: Die Definition macht nämlich nebenbei auch eine Aussage! Aus der Schule wissen wir, daß es Funktionen gibt, deren Ableitung nicht existiert, weil sie z.B. einen Knick haben. Die oben angegebene „Definition" tut aber so, als ob *jede* Funktion eine Ableitung hätte, die man als den beschriebenen Grenzwert definiert.

Die Vermischung von Definitionen und Aussagen ist durchaus üblich, kann aber verwirrend sein und erfordert besondere Sorgfalt.

3.b Vermutungen und Sätze

Eine *mathematische Vermutung* macht über zuvor definierte mathematische Objekte präzise Aussagen. Dabei verknüpft sie in der Regel verschiedene Definitionen.

3.b.1 Positive Beispiele

Angenommen, wir haben definiert, wann eine natürliche Zahl n durch eine andere natürliche Zahl k teilbar ist. Dann sind folgende Aussagen mathematische Vermutungen:

Vermutung 3(8). Jede durch 4 teilbare Zahl ist auch durch 2 teilbar.

Vermutung 3(9). Jede durch 4 teilbare Zahl ist auch durch 3 teilbar.

Vermutung 3(10). Sei n eine natürliche Zahl. Dann ist n durch 3 teilbar oder n ist nicht durch 3 teilbar.

Vermutung 3(11). Sei n eine natürliche Zahl. Dann ist n durch 3 teilbar und n ist nicht durch 3 teilbar.

3.b.2 Negative Beispiele

Vermutung 3(12). Sei r eine rationale Zahl. Dann ist r durch 3 teilbar.

Für rationale Zahlen, die nicht zufällig natürliche Zahlen sind, ist „durch 3 teilbar" gar nicht definiert.

Vermutung 3(13). Es gibt mehr natürliche Zahlen als Primzahlen.

Der Begriff „mehr" ist bei unendlichen Mengen a priori nicht definiert. (Man kann auch unendliche Mengen sinnvoll vergleichen; dies betrachtet man in Analysis I).

Vermutung 3(14). Es gibt eine natürliche Zahl n, die größer ist als mein Kontostand.

Kein Kommentar.

3.b.3 Von einer Vermutung zu einem Satz

Mathematische Vermutungen sind grundsätzlich entweder *wahr* oder *falsch*. Jede Vermutung hat genau eine *gegenteilige Vermutung*, die dann falsch ist, wenn die ursprüngliche wahr ist und umgekehrt. Die gegenteilige Vermutung zu 3(8) wäre

Vermutung 3(15). Es gibt eine durch 4 teilbare Zahl, die *nicht* durch 2 teilbar ist.

Ziel eines Mathematikers ist es, Vermutungen aufzustellen und auf ihren Wahrheitsgehalt hin zu überprüfen. Dies macht man mit Hilfe des im nächsten Abschnitt angesprochenen *Beweises*. Gibt es zu einer Vermutung einen Beweis, so heißt die Vermutung *Satz*.

Nebenbei bemerkt: Sätze heißen nicht immer Sätze. Folgende Begriffe treten auch auf:

- **Lemma:** Ein Lemma ist eine Aussage, die nur für den/die folgenden Sätze benutzt wird, aber ansonsten nicht von Belang ist.
- **Korollar:** Ein Korollar ist eine Aussage, die (mehr oder weniger) direkt aus der Aussage des Satzes folgt. Es ist also weder ein langer Beweis noch eine neue Definition erforderlich.

3.c Beweise

Beweise bilden den Hauptteil der kreativen Arbeit eines Mathematikers. Entgegen der landläufigen Meinung ist es nämlich nicht die Hauptaufgabe eines Mathematikers zu rechnen, sondern zu beweisen.

Sagen wir nun, wir wollen eine Aussage A beweisen. Dann prüfen wir zuerst, daß es sich bei A um eine korrekt formulierte mathematische Vermutung handelt, d.h. daß alle verwendeten Begriffe definiert sind, und die Aussage präzise formuliert.

Ein *Beweis* fängt immer an bei bereits bekannten (und bewiesenen) Sätzen. Aus diesen wird nun in logisch einwandfreien Schritten die Aussage der Vermutung gefolgert. Gelingt dies, so wird aus der Vermutung ein *Satz*.

3.c.1 Positive Beispiele

Angenommen, der folgende Satz wurde schon bewiesen:

Satz 3(16). Ist eine natürliche Zahl p durch eine natürliche Zahl k teilbar, so ist auch $p \cdot q$ durch k teilbar (für jede natürliche Zahl q).

Dann sind folgende Abschnitte ordentliche Beweise:

Satz 3(17). Jede durch 4 teilbare Zahl ist auch durch 2 teilbar.

Beweis. Sei n eine durch 4 teilbare Zahl. Setzen wir $k = 4$, so folgt nach Definition 3(5), daß es eine Zahl q gibt mit $n = 4 \cdot q$.

Da die Zahl 4 durch 2 teilbar ist, ist auch $4 \cdot q$ durch 2 teilbar (Siehe Satz 3(16)). Damit ist der Satz gezeigt. □

Satz 3(18). Es gilt *nicht*: Jede durch 4 teilbare Zahl ist durch 3 teilbar.

Beweis. Die Zahl 8 ist durch 4 teilbar, aber nicht durch 3. Daher ist nicht *jede* durch 4 teilbare Zahl durch 3 teilbar. Der Satz ist also gezeigt. □

Das Gegenteil einer Aussage „Jede…" ist also eine Aussage der Form „Es gibt eine, … so daß *nicht* …".

3.c.2 Negative Beispiele

Satz 3(19). Jede durch 4 teilbare Zahl ist auch durch 2 teilbar.

Beweis. Sei n durch 4 teilbar. Sei k die größte gerade Zahl, die n teilt. Dann gibt es nach Satz 3(5) eine Zahl q mit $n = k \cdot q$. Die 2 steckt nun in der geraden Zahl k, also auch in n. □

Zu ungenau; der relevante Satz wird nicht zitiert. Stattdessen wird „anschaulich" argumentiert.

Satz 3(20). Jede durch 4 teilbare Zahl ist auch durch 2 teilbar.

Beweis. Mein iPhone hat dies für alle Fälle kleiner als 10^{12} durchgerechnet. □

Die Behauptung *Alle Zahlen sind kleiner als* 10^{13} läßt sich leicht für alle Zahlen kleiner als 10^{12} überprüfen…

Mehr Beispiele finden sich in Abschnitt 4.

4 Beweismethoden

Letztendlich lassen sich Beweise nicht mechanisch führen; es braucht immer den Einfallsreichtum des Mathematikers. Dennoch gibt es einige hilfreiche Methoden, wie sich ein vernünftiger Beweis aufbauen läßt.

Die wichtigsten sollen im Folgenden vorgestellt werden:

4.a Beweis durch Widerspruch

Eine Vermutung ist immer entweder *wahr* oder *falsch*. Zu jeder Vermutung A gibt es weiterhin eine gegenteilige Aussage, die wir *(nicht A)* nennen. Sie ist genau dann falsch, wenn die ursprüngliche Aussage wahr ist (und umgekehrt). Ein wichtiges mathematisches Prinzip ist:

Prinzip. *Läßt sich aus einer mathematischen Aussage eine falsche Aussage herleiten, dann ist die Aussage selbst falsch.*

Daraus läßt sich folgendes Beweisgerüst ableiten:

Satz 4(1). Es gilt A.

Beweis. Sei B die Aussage *(nicht A)*.

Angenommen, es gilt B. Nun folgern wir Schritt für Schritt aus B weitere Aussagen, solange bis man auf eine Aussage stößt, die schon als falsch bekannt ist.

Jetzt wissen wir: B ist falsch. Also muß A gelten. □

Folgende Beispiele sollen dies illustrieren:

Satz 4(2). Es gibt keine kleinste positive rationale Zahl.

Beweis. Wir nehmen also das Gegenteil an: Es *gibt* eine kleinste positive rationale Zahl.

Sei q die kleinste positive rationale Zahl. Dann ist $q/2$ auch eine positive rationale Zahl. Da q die kleinste positive rationale Zahl ist, gilt:

$$\frac{q}{2} \geq q$$

Division durch q (erlaubt, weil $q \neq 0$) ergibt:

$$\frac{1}{2} \geq 1$$

Die letzte Aussage ist bekanntermaßen falsch. Daher konnten wir aus der Aussage „Es gibt eine kleinste positive rationale Zahl" eine falsche Aussage herleiten. Die Aussage selbst muß daher falsch sein. □

Ein *Widerspruch* ist logisch gesehen eine Aussage der Form:

Es gilt *A*, und es gilt *(nicht A)*.

Beispielsweise eben: Es gilt $a > b$ und es gilt $a \leq b$. Widersprüche sind naturgemäß immer falsche Aussagen.

Beachte außerdem: Wir wissen zwar, daß eine Aussage falsch ist, wenn aus ihr etwas falsches folgt. Andersherum ist eine Aussage aber nicht dadurch wahr, daß etwas wahres aus ihr folgt! Aus $1 = 2$ lassen sich viele Aussagen folgern, manche davon sind wahr, manche falsch.

4.b Beweis mit Fallunterscheidung

Häufig ist es sinnvoll, ein Problem in mehrere Fälle zu unterteilen, die man einzeln untersucht. Mathematisch gesehen heißt das, daß folgende Sätze äquivalent (gleichwertig) sind:

Satz 4(3). Es gilt *A*.

Satz 4(4). Unter der Voraussetzung *B* gilt *A* und unter der Voraussetzung *(nicht B)* gilt *A*.

Unterscheiden wir mehr als zwei Fälle, so brauchen wir noch ein *C*, *D* usw. und müssen am Schluß *(nicht B) und (nicht C) und* .. betrachten.

Ein Beispiel:

Satz 4(5). Wenn ich von einer ungeraden Quadratzahl 1 subtrahiere, so ist das Ergebnis stets durch 8 teilbar.

Beweis. Sei q^2 eine Quadratzahl. Dann läßt sich $q^2 - 1$ nach der binomischen Formel als $(q-1)(q+1)$ faktorisieren. Wir unterscheiden nun drei Fälle:

1. $q-1$ **ist durch 4 teilbar:** Dann ist $q+1$ gerade, da es genau 2 größer ist. Das Produkt einer geraden und einer durch 4 teilbaren Zahl ist durch 8 teilbar (siehe z.B. Satz über eindeutige Primfaktorzerlegung).

2. $q+1$ **ist durch 4 teilbar:** Dann ist $q-1$ gerade, da es genau 2 kleiner ist. Nun argumentiert man wie in Fall 1.

3. **Weder** $q-1$ **noch** $q+1$ **sind durch 4 teilbar:** Wir wissen nach Voraussetzung, daß q^2 ungerade ist. Somit ist auch q ungerade (Beweis durch Widerspruch: Wäre q gerade, so wäre q^2 gerade.). Da q ungerade ist, sind $q+1$ und $q-1$ gerade. Nun ist aber genau jede zweite gerade Zahl durch 4 teilbar (dies läßt sich einfach mit Modulo-Rechnung beweisen, siehe Abschnitt 5). Somit ist entweder $q-1$ oder $q+1$ durch 4 teilbar. Der dritte Fall tritt also nie ein.

□

Wichtig ist bei einer Fallunterscheidung, daß sie immer *vollständig* ist, d.h. alle denkbaren Fälle abdeckt. Die Vollständigkeit muß im Zweifelsfall auch bewiesen werden; dies haben gerade durch die Betrachtung des dritten Falles gemacht.

Auch wenn wir reelle und irrationale Zahlen noch nicht formal definiert haben, werden wir für den folgenden Satz einmal so tun. Wir setzen dabei voraus, daß es sich bei $\sqrt{2}$ um eine irrationale Zahl handelt.

Satz 4(6). Es gibt zwei irrationale Zahlen a und b, so daß a^b eine rationale Zahl ist.

Beweis. Wir unterscheiden zwei Fälle:

1. $\sqrt{2}^{\sqrt{2}}$ ist eine rationale Zahl: In diesem Fall setzen wir $a = b = \sqrt{2}$ und haben das Problem gelöst.

2. $\sqrt{2}^{\sqrt{2}}$ ist *keine* rationale Zahl: Dann handelt es um eine irrationale Zahl. Wir setzen $a = \sqrt{2}^{\sqrt{2}}$ und $b = \sqrt{2}$. Dann gilt nach den Potenzregeln:

$$a^b = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^2 = 2$$

   Somit erfüllen diese a und b die gewünschten Bedingungen.

□

Bei diesem Beweis handelt es sich um eine vollständige Fallunterscheidung, obwohl wir letzendlich nicht sagen können, welcher der Fälle überhaupt eintritt. Der Satz ist bewiesen; der Beweis gibt uns jedoch keinen Anhaltspunkt, wie wir a und b tatsächlich finden.

4.c Beweis durch Induktion

(nach einem Skript von Lars Scheele)

4.c.1 Der Irrtum von Fermat

PIERRE DE FERMAT (ein berühmter französischer Mathematiker) betrachtete Zahlen der Form

$$F_n = 2^{2^n} + 1 \qquad n \in \mathbb{N}$$

Die ersten dieser Zahlen lauten:

$$\begin{aligned} F_0 &= 3 \\ F_1 &= 5 \\ F_2 &= 17 \\ F_3 &= 257 \\ F_4 &= 65537 \end{aligned}$$

Dies sind alles Primzahlen und so vermutete Fermat im Jahre 1637, daß alle weiteren Zahlen dieser Form ebenfalls Primzahlen seien.

Ein solcher Schluß wird in der Logik „Induktion" genannt: man schließt von einer Teilmenge an Beispielen auf die Gesamtheit. Induktionsschlüsse sind im Alltag weit verbreitet: „Morgen wird die Sonne aufgehen, weil sie es heute tat und gestern und vorgestern..."

Logisch gesehen sind solche Schlüsse allerdings nicht zulässig! Selbst wenn man noch so viele Beispiele kennt, zeigt dies nicht den allgemeinen Fall. Der Satz: „Alle Menschen sind weiblich." ist mit Sicherheit falsch und doch gibt es sehr viele Beispiele, die diese Behauptung stützen können.

Ähnlich verhält es sich auch mit den Fermat-Zahlen. Etwa 100 Jahre nach der Vermutung entdeckte EULER im Jahre 1732, daß die nächste Fermat-Zahl keine Primzahl ist:

$$F_5 = 4294967297 = 641 \cdot 6700417$$

Inzwischen wird sogar vermutet, daß alle weiteren Fermat-Zahlen F_n mit $n \geq 5$ **keine** Primzahlen sind, aber ein formaler Beweis steht bislang noch aus.

4.c.2 Vollständige Induktion

Wir wollen hier ein anderes Beispiel betrachten. Schauen wir uns die Summen der ersten n ungeraden Zahlen an:

$$\begin{aligned} 1 &= 1 \\ 4 &= 1+3 \\ 9 &= 1+3+5 \\ 16 &= 1+3+5+7 \\ 25 &= 1+3+5+7+9 \end{aligned}$$

Es fällt auf, daß auf der linken Seite stets eine Quadratzahl steht. Diese Vermutung kann man mit Hilfe der Summennotation allgemein für beliebiges $n \in \mathbb{N}$ formulieren:

Vermutung 4(7). Für alle $n \in \mathbb{N}$ gilt:

$$\sum_{k=1}^{n} (2k-1) = n^2$$

Dabei bedeutet

$$\sum_{k=1}^{n} \big[\text{Ausdruck, der } k \text{ enthält}\big],$$

daß wir nacheinander $k = 1$, $k = 2$, usw. bis $k = n$ setzen und alles dies zusammenrechnen. Programmiertechnisch würde das etwa so aussehen (Wenn x die Summe bezeichnet):

```
x=0
FOR k=1 TO n DO
x = x + (2k-1)
NEXT
```

Für $n \in \{1,2,3,4,5\}$ haben wir uns schon von der Richtigkeit der Vermutung überzeugt. Aber das Beispiel der Fermat-Zahlen lehrt uns, daß dies noch kein Beweis für die Richtigkeit der allgemeinen Vermutung ist. Und natürlich kann man nicht alle Fälle nachrechnen, weil es unendlich viele sind. Was ist der Ausweg aus diesem Dilemma?

Die Lösung des Problems ist ein Beweisverfahren, das unter dem Namen „vollständige Induktion" bekannt ist. Gegeben ist eine Aussage in Abhängigkeit von n, sagen wir $A(n)$. In unserem Fall ist also $A(n)$ die Aussage

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

Für gegebenes $n \in \mathbb{N}$ kann $A(n)$ wahr oder falsch sein. Wir haben uns oben davon überzeugt, daß $A(1)$ bis $A(5)$ wahr sind, möchten aber gern beweisen, daß $A(n)$ für alle $n \in \mathbb{N}$ eine wahre Aussage darstellt. Die vollständige Induktion geht nun in zwei Schritten vor:

1) *Der Induktionsanfang:* Man beweist, daß $A(1)$ gilt.

2) *Der Induktionsschritt:* Man beweist: falls für ein $n \in \mathbb{N}$ die Aussage $A(n)$ wahr ist, dann auch die Aussage $A(n+1)$.

Der Trick besteht also darin, daß man im Induktionsschritt von der Aussage für ein *beliebiges* $n \in \mathbb{N}$ auf den Nachfolger $n+1$ schließt. Hat man beide Schritte gezeigt, ist man fertig und hat bewiesen, daß die Aussage für alle $n \in \mathbb{N}$ gilt.

Im Detail stelle man sich das so vor: Der Induktionsanfang beinhaltet die Wahrheit der Aussage $A(1)$. Jetzt wenden wir den Induktionsschritt für $n = 1$ an und erhalten, daß $A(2)$ eine wahre Aussage ist. Jetzt aber können wir wieder den Induktionsschritt für $n = 2$ anwenden und erhalten $A(3)$ und so weiter.

Ein hilfreiches Bild ist vielleicht das Folgende: man stelle sich die Aussagen wie Dominosteine vor, die aneinander gereiht sind. Wenn ein Dominostein umfällt, dann soll das bedeuten, daß die Aussage wahr ist. Der Induktionsschritt formuliert nun das Gesetz, daß ein fallender Dominostein seinen Nachbarn umstößt. (Wenn $A(n)$ gilt, dann auch $A(n+1)$.) Und der Induktionsanfang garantiert uns das Fallen des ersten Steins – und damit fallen alle um.

Soweit die graue Theorie. Widmen wir uns dem Beweis der obigen Vermutung – der Induktionsanfang ist geleistet, wir haben uns davon überzeugt, daß $A(1)$ wahr ist. Kommen wir also zum Induktionsschritt:

Beweis. Sei $n \in \mathbb{N}$ beliebig, so daß $A(n)$ wahr ist, d.h. es gelte

$$\sum_{k=1}^{n} (2k-1) = n^2$$

Zu zeigen ist, daß aus dieser Voraussetzung $A(n+1)$ folgt. Rechnen wir das nach:

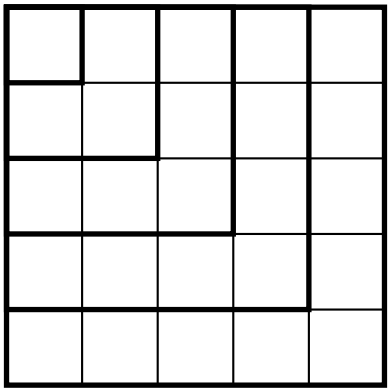
$$\sum_{k=1}^{n+1} (2k-1) = \sum_{k=1}^{n} (2k-1) + \big(2(n+1)-1\big) \overset{IV}{=} n^2 + 2n + 1 = (n+1)^2$$

□

Das kleine „IV" (Induktionsvoraussetzung) deutet die Stelle an, an der benutzt wird, daß $A(n)$ laut Annahme gilt.

Zusammenfassend kann man sagen, daß der eigentliche Trick der Induktion darin besteht, den Schluss von einer Zahl auf ihren Nachfolger allgemein zu formulieren, so daß dieser im Prinzip beliebig oft anwendbar ist.

Zum Schluß noch eine geometrische Anschauung der soeben bewiesenen Formel:



Beginnend mit einem Kästchen in der oberen linken Ecke, wird immer eine ungerade Anzahl an Kästchen hinzugefügt und es entsteht jeweils wieder ein Quadrat.

4.c.3 Der kleine Gauß

Es wird eine Anekdote über den deutschen Mathematiker CARL-FRIEDRICH GAUSS erzählt, der, weil er die anderen Aufgaben schon gelöst hatte, die Aufgabe erhält, die natürlichen Zahlen von 1 bis 100 alle aufzuaddieren. Die abkürzende Notation benutzend sollte also die Summe

$$\sum_{i=1}^{100} i$$

berechnet werden.

Laut der Anekdote soll der „kleine Gauß" seinen Lehrer damit überrascht haben, in kürzester Zeit auf das (korrekte) Ergebnis 5050 zu kommen.

Aufgrund dieser Anekdote, deren Wahrheitsgehalt ungewiß ist, trägt die folgende Formel den Namen „Gaußsche Summenformel" oder manchmal auch einfach „der kleine Gauß":

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

Für $n = 100$ ergibt sich gerade $\frac{100 \cdot 101}{2} = 50 \cdot 101 = 5050$. Der Beweis der Formel funktioniert über vollständige Induktion.

Beweis.

a) *Induktionsanfang:* Sei $n = 1$. Dann steht auf der linken Seite $\sum_{i=1}^{1} i = 1$ und auf der rechten gerade

$$\frac{1 \cdot 2}{2} = 1$$

Die Aussage ist also für $n = 1$ wahr.

b) *Induktionsschritt:* Die Aussage gelte für $n \in \mathbb{N}$. Es folgt:

$$\sum_{i=1}^{n+1} i = \sum_{i=1}^{n} i + (n+1) \overset{IV}{=} \frac{n \cdot (n+1)}{2} + \frac{2n+2}{2} = \frac{n^2+3n+2}{2}$$

Andererseits gilt aber

$$\frac{(n+1)(n+2)}{2} = \frac{n^2+3n+2}{2}$$

Dies zeigt die Behauptung.

□

4.c.4 Alle Dinge sind gleich

Zum Schluß des Kapitels über vollständige Induktion noch eine kleine Warnung: Manchmal muss man bei solchen Beweisen sehr genau hinschauen, sonst können sich Fehler einschleichen. Wir werden nun eine offensichtlich falsche Aussage mit vollständiger Induktion beweisen. Die Aussage lautet:

„Alle Studierenden an der Universität Bielefeld studieren das Gleiche."

Um diese Aussage mit Induktion angehen zu können, muß noch eine natürliche Zahl n irgendwo auftauchen. Daher wird die Aussage in Abhängigkeit von n wie folgt umformuliert:

„In einer beliebigen Menge von n Studierenden studieren alle das Gleiche."

Dies soll die Aussage $A(n)$ sein, die im Folgenden mit vollständiger Induktion bewiesen wird.

Beweis.

a) *Induktionssanfang:* Sei $n = 1$. In einer beliebigen Menge, die nur einen Studenten oder eine Studentin enthält, ist die Aussage klar.

b) *Induktionsschritt:* Nehmen wir an, die Aussage sei für $n \in \mathbb{N}$ bewiesen. Wir nehmen uns nun eine beliebige Menge M her, in der $n+1$ Studierende sind und wollen zeigen, daß die alle das Gleiche studieren. Diese $n+1$ Studierenden sollen im Folgenden $a_1, a_2, \ldots, a_{n+1}$ heißen. In Mengenschreibweise heißt dies:

$$M = \{a_1, a_2, \ldots, a_{n+1}\}$$

Betrachten wir nun eine Teilmenge von M, in welcher der erste Studierende fehlt:

$$M' = \{a_2, a_3, \ldots, a_{n+1}\}$$

M' enthält nur n Studierende und die studieren nach Induktionsvoraussetzung alle das Gleiche. Fehlt noch a_1 – aber zu diesem Zweck betrachten wir eine zweite Teilmenge:

$$\tilde{M} = \{a_1, a_2, \ldots, a_n\}$$

Auch in dieser Menge sind nur n Studierende enthalten, die wieder nach Induktionsvoraussetzung alle das Gleiche studieren. Nehmen wir uns nun ein beliebiges Element a_k aus dem Schnitt (also ein a_k aus der Menge $\{a_2, \ldots, a_n\}$), so folgt, daß a_1 das Gleiche studiert wie a_k und a_k das Gleiche wie a_{n+1}, denn a_1 und a_k liegen in $\tilde{M}$ und a_k und a_{n+1} liegen in M'.

Damit ist die Aussage bewiesen und alle Studierenden aus M studieren das Gleiche.

□

Da an der Universität nur endlich viele Studierende eingeschrieben sind, muss man n nur groß genug wählen und die Aussage $A(n)$ für dieses n zeigt die Behauptung.

Natürlich kann man diesen Beweis nun für beliebige Dinge führen: Alle Bücher heißen gleich, alle Menschen haben das gleiche Geschlecht, alle Häuser sind gleich hoch ... wo genau der Fehler der obigen Argumentation liegt, wird in den Übungen besprochen.

5 Restklassenrechnung und Wohldefiniertheit

Ein wichtiges Grundprinzip der Mathematik ist das der *Äquivalenzklasse*. Mathematische Objekte (wie auch Gegenstände des Alltags) sind bei näherer Betrachtung häufig über alle Maßen komplex und unübersichtlich. Schauen wir uns z.B. einen Stuhl an, so besteht er (häufig) aus Holz und Leim, welches sich wiederum in unterschiedliche Strukturen bis herunter zu Molekülen, Atomen und Quarks zerlegen läßt. Meistens sagt man jedoch nicht „Ich suche einen Gegenstand mit etwa 10^{14} Kohlenstoffatomen", sondern eher: „Ich suche einen Gegenstand, auf dem man (halbwegs bequem) sitzen kann". Mathematisch ausgedrückt: Um zu entscheiden, ob man auf einem Gegenstand sitzen kann, interessiert mich nur, daß er der Äquivalenzklasse *Stuhl* angehört, nicht jedoch seine Feinstruktur.

Eine Art, Zahlen in Äquivalenzklassen einzuteilen, werden wir im folgenden behandeln:

5.a Restklassenrechnung

Wenn man eine Eigenschaft für alle natürlichen Zahlen überprüfen möchte, dann stößt man immer wieder auf das Problem: Es sind unendlich viele. Wir können leider nicht jede einzelne anschauen. Eine Methode, solch ein Problem zu behandeln, ist die vollständige Induktion. In Teilbarkeitsfragen bietet sich aber häufig eine andere Methode an. Dies wollen wir am Beispiel „Teilen durch 5" einmal genauer betrachten.

Die meisten natürlichen Zahlen lassen sich nicht glatt durch 5 teilen. Es bleibt ein *Rest*: Dieser ist 0 (wenn es „aufgeht"), 1, 2, 3 oder 4. Diese Reste definieren unsere Äquivalenzklassen: Jede natürliche Zahl gehört entweder in die Klasse [0], [1], [2], [3] oder [4], je nachdem, welchen Rest sie beim Teilen durch 5 läßt. Diese nennt man *Restklassen modulo 5*.

Die Notation [1] bezeichnet also nicht eine einzelne Zahl, sondern eine *Menge von Zahlen*, nämlich

$$[1] = \{\ldots, -9, -4, 1, 6, 11, \ldots\}.$$

Insgesamt haben wir damit die ganzen Zahlen in fünf Mengen aufgeteilt, so daß jede Zahl in genau einer der Mengen enthalten ist.

Für unsere fünf Objekte $[0], [1], [2], [3], [4]$ wollen wir nun eine Addition $\boxplus$ einführen. Wir wollen also für jede zwei Zahlen m, n zwischen 0 und 4 (einschließlich) eine Zahl k angeben und dann schreiben:

$$[m] \boxplus [n] = [k].$$

Man könnte diese Addition nun auf ganz verschiedene Weise definieren, z.B. so, daß die Summe zweier Restklassen immer [0] ist. Damit uns diese Addition aber etwas nützt, wollen wir, daß sie folgende Eigenschaft erfüllt:

Addieren wir zwei ganze Zahlen a und b, so soll die Summe ihrer Restklassen gleich der Restklasse ihrer Summe sein.

Betrachten wir ein Beispiel: Sei $a = 1$ und $b = 3$. Dann ist die Restklasse der Summe [4]. Dann soll die Summe der Restklassen $[1] \boxplus [3]$ auch [4] sein. Wir überlegen uns daher folgende Definition:

Definition 5(1). Sei k der Rest von $m+n$ beim Teilen durch 5. Dann ist $[m] \boxplus [n]$ definiert als $[k]$.

Es gilt also $[3] \boxplus [4] = [2]$ oder $[2] \boxplus [3] = [0]$.

In Zukunft wollen wir etwas weniger streng sein und erlauben auch Schreibweisen wie [7], was dann das gleiche wie [2] meint (Rest von 7 beim Teilen durch 5).

Genauso können wir folgendes definieren:

Definition 5(2). Sei k der Rest von $m-n$ beim Teilen durch 5. Dann ist $[m] \boxminus [n]$ definiert als $[k]$.

Definition 5(3). Sei k der Rest von $m \cdot n$ beim Teilen durch 5. Dann ist $[m] \boxtimes [n]$ definiert als $[k]$.

Auf die Division verzichten wir erst einmal.

Schauen wir uns stattdessen ein paar Beispiele an, in denen Restklassenrechnung (bezüglich anderer Teiler als 5) nützlich sein kann.

5.a.1 Anwendungen

Wir wollen nun sehen, daß Restklassenrechnung sinnvoll zur Lösung von Aufgaben sein kann. Daher betrachten wir die folgende Fragen:

Aufgabe 5(4). Ist die Zahl $111111111\ldots111111111111$ eine Quadratzahl für irgendeine Anzahl an Einsen?

Bestimmen wir zuerst die Klasse dieser Zahl beim Teilen durch 4. Da alle Vielfache von 100 durch 4 teilbar sind, sehen wir (wenn $[]_4$ die Restklasse beim Teilen durch 4 bezeichnet):

$$[111111111\ldots1111111]_4 = [11]_4 = [3]_4.$$

Nun überprüfen wir, ob eine Quadratzahl in der Klasse $[3]_4$ liegen kann. Da Multiplikation mit der Bildung von Restklassen verträglich ist, reicht es dafür, alle Klassen (also $[0]_4$, $[1]_4$, $[2]_4$ und $[3]_4$) zu überprüfen:

a	a^2
$[0]_4$	$[0]_4$
$[1]_4$	$[1]_4$
$[2]_4$	$[0]_4$
$[3]_4$	$[1]_4$

Wir sehen also, daß Quadratzahlen nicht in der Klasse $[3]_4$ liegen können. Damit kann $111111\ldots111111$ nie eine Quadratzahl sein.

Aufgabe 5(5). Sei $Q(n)$ definiert als die Quersumme (Summe aller Ziffern) der natürlichen Zahl n. Bestimme

$$Q\Big(Q\Big(Q\big(4444^{4444}\big)\Big)\Big)$$

Machen wir zunächst eine Abschätzung: $4444^{4444} < 10000^{10000} = 10^{40000}$. Daher hat die Zahl höchstens 40000 Stellen, die jeweils maximal die Ziffer 9 enthalten. Es ist also

$$Q\left(4444^{4444}\right) < 40000 \cdot 9 = 360000.$$

Ist eine Zahl kleiner als 360000, so ist ihre Quersumme maximal $2 + 5 \cdot 9$, also 47. Daher

$$Q\left(Q\left(4444^{4444}\right)\right) \leq 47.$$

Damit ist aber

$$Q\left(Q\left(Q\left(4444^{4444}\right)\right)\right) \leq 12.$$

Somit bleiben für unser Ergebnis nur noch 12 verschiedene Möglichkeiten übrig. Wichtig ist nun folgende Eigenschaft:

Die Quersumme einer Zahl hat beim Teilen durch 9 den gleichen Rest wie die Zahl selbst.

Wenden wir dieses Argument mehrmals an, so wissen wir, daß

$$\left[Q\left(Q\left(Q\left(4444^{4444}\right)\right)\right)\right]_9 = \left[4444^{4444}\right]_9.$$

Es lohnt sich also, die rechte Seite dieser Gleichung genauer zu bestimmen. Es gilt $[4444]_9 = [7]_9$. Betrachten man die Reihe der Potenzen, so ergibt sich folgendes Bild

$[7]_9$	$[7]_9^2$	$[7]_9^3$	$[7]_9^4$	$[7]_9^5 \ldots$
$[7]_9$	$[4]_9$	$[1]_9$	$[7]_9$	$[4]_9 \ldots$

Die Potenzen wiederholen sich also mit einer Periode von 3. Daher ist $[7]^{4444} = [7]^1 = [7]$. Eine formale Rechtfertigung dafür, daß wir 4444 einfach durch 7 ersetzen können, wird im nächsten Abschnitt gegeben.

Wir wissen also, daß die gesuchte Zahl kleiner oder gleich 12 ist und gleichzeitig Rest 7 beim Teilen durch 9 läßt. Daher muß obige Quersumme gleich 7 sein.

Wir wollen nun das ganze von einem abstrakteren Standpunkt betrachten und dafür *Äquivalenzrelationen* einführen.

5.b Äquivalenzrelationen

Wir betrachten eine Menge M, z.B. $M = \mathbb{Z}$. Eine Relation $\sim$ sagt, ob eine bestimmte Beziehung zwischen zwei Elementen a und b der Menge M besteht, d.h. wenn diese Beziehung besteht, dann schreiben wir $a \sim b$, ansonsten $a \not\sim b$. Wichtige Beispiele für Relationen sind $=$, $<$, oder $|$ (teilt): Wenn zwei natürliche Zahlen a und b gegeben sind, so gilt entweder $a = b$ oder $a \neq b$. Genauso gilt entweder $a < b$ oder $a \not< b$, was man normalerweise als $a \geq b$ schreibt.

Es gibt sehr verschiedene Arten von Relationen. Uns interessieren vor allem Relationen, die sich ähnlich verhalten wie $=$. Dies nennt man *Äquivalenzrelationen*. Formal sind sie auf folgende Weise definiert:

Definition 5(6). Eine Relation $\sim$ auf einer Menge M heißt Äquivalenzrelation, wenn Folgendes für alle $a, b, c \in M$ gilt:

1. Aus $a \sim b$ folgt $b \sim a$ (Symmetrie).
2. Aus $a \sim b$ und $b \sim c$ folgt $a \sim c$ (Transitivität).
3. Es gilt $a \sim a$ (Reflexivität).

Setzt man $\sim$ gleich $=$, so erkennt man schnell, daß alle diese Bedingungen erfüllt sind. Die Relationen $<$ und $|$ sind allerdings keine Äquivalenzrelationen (beiden fehlt es an der Symmetrie).

Bisher kennen wir noch keine interessante Äquivalenzrelation; wir können aber auch unsere Restklassen über eine Äquivalenzrelation definieren.

Definition 5(7). Es sei $a \sim_5 b$, falls $a - b$ durch 5 teilbar ist. Ansonsten $a \not\sim_5 b$.

Überprüfen wir nun die Bedingungen:

1. Wenn $a - b$ durch 5 teilbar ist, so auch $b - a$. Damit ist die Relation $\sim_5$ symmmetrisch.
2. Wenn $a - b$ und $b - c$ durch 5 teilbar sind, so auch $(a - b) + (b - c) = a - c$. Damit ist auch $a \sim_5 c$ und die Relation $\sim_5$ ist transitiv.
3. $a - a = 0$ ist immer durch 5 teilbar.

Wir haben also eine weitere Äquivalenzrelation gefunden.

Sei nun $\overline{a}$ die Menge aller $c \in \mathbb{Z}$, für die gilt $a \sim_5 c$. Diese nennen wir die zu a gehörende *Äquivalenzklasse*.

Lemma 5(8).

(i) Sind a, b Elemente von $\mathbb{Z}$, so gilt entweder $\overline{a} = \overline{b}$, oder $\overline{a}$ und $\overline{b}$ haben keine Elemente gemeinsam.

(ii) Jedes Element von $\mathbb{Z}$ liegt genau in einer Äquivalenzklasse.

Beweis. (i) Wir unterscheiden zwei Fälle:

(a) $a \sim_5 b$: Wir wollen zeigen, daß $\overline{a} = \overline{b}$. Dafür müssen wir zeigen, daß aus $a \sim_5 c$ immer $b \sim_5 c$ folgt und umgekehrt.
Nehmen wir also an, es gilt $a \sim_5 c$. Nun gilt auch $b \sim_5 a$ (nach Symmetrie aus $a \sim_5 b$). Nutzt man nun die Transitivität, so folgt aus $b \sim_5 a$ und $a \sim_5 c$ nun $b \sim_5 c$, wie gewünscht. Andersherum argumentiert man genauso. Damit ist der erste Fall gezeigt.

(b) $a \not\sim_5 b$: Wir führen einen Beweis durch Widerspruch.
Angenommen c liegt in $\overline{a}$ und in $\overline{b}$. Dann gilt $a \sim_5 c$ und $b \sim_5 c$. Nach Symmetrie gilt auch $c \sim_5 b$. Verknüpft man dies nach der Transitivität, so folgt $a \sim_5 b$. Dies widerspricht jedoch $a \not\sim_5 b$, womit die Annahme nicht zutreffen kann. Somit haben $\overline{a}$ und $\overline{b}$ keine Elemente gemeinsam.

(ii) Zuerst einmal stellen wir fest: Jedes Element a leigt in *mindestens* einer Äquivalenzklasse, nämlich $\overline{a}$. Liegt a auch in $\overline{b}$, so haben $\overline{a}$ und $\overline{b}$ mindestens ein Element gemeinsam: Nach (i) müssen sie also gleich sein.

Anmerkung: Dieser Beweis funktioniert genauso für jede andere Äquivalenzrelation. □

Lemma 5(9). Die durch $\overline{a}$ definierten Klassen entsprechen genau den durch [0], [1], usw. definierten Klassen.

Beweis. In den Übungen. □

5.b.1 Rechnen „modulo 5"

Wir wollen nun mit den Äquivalenzklassen rechnen. Dabei gehen wir wie bei den oben definierten Restklassen $[a]$ vor, werden die Eigenschaften dieses Mal aber formal beweisen.

Definition 5(10). Die Addition von Restklassen ist auf folgende Weise definiert:

$$\overline{a} + \overline{b} := \overline{a + b}.$$

Es gilt also z.B. $\overline{6}+\overline{7}=\overline{13}$. Wir müssen jedoch mit der gerade gemachten Definition sehr vorsichtig sein. Jede Äquivalenzklasse hat ja viele verschiedene Elemente (auch Repräsentanten genannt). Wollen wir nun $\overline{6}+\overline{7}$ ausrechnen, so könnten wir auch erst $\overline{6}$ durch $\overline{21}$ ersetzen, da 6 und 21 die gleiche Äquivalenzklasse repräsentieren. Nun steht dort $\overline{21}+\overline{7}=\overline{28}$. Wir haben Glück: Weil $28-13=15$ durch 5 teilbar ist, repräsentiert das neue Ergebnis die gleiche Äquivalenzklasse wie das alte. Dies müssen wir aber noch allgemein überprüfen.

Prinzip. *Eine Definition, die eine Äquivalenzklasse $\overline{a}$ benutzt, heißt* wohldefiniert, *falls sie nicht davon abhängt, welchen Repräsentanten aus $\overline{a}$ man auswählt. Anders ausgedrückt: Ist $\overline{a}$ gleich $\overline{b}$, so darf das Ergebnis der Definition nicht davon abhängen, ob man a oder b einsetzt.*

Eine Definition, die Äquivalenzklassen benutzt, wird erst dann zu einer richtigen Definition, wenn man die Wohldefiniertheit überprüft hat. Tun wir dies also für obiges Beispiel:

Lemma 5(11). Ist $\overline{a}$ gleich $\overline{a}_2$ und $\overline{b}$ gleich $\overline{b}_2$, so folgt $\overline{a+b}=\overline{a_2+b_2}$.

Beweis. Nach Definition der Äquivalenzklassen wissen wir: Es gibt Zahlen k_a und k_b mit $a-a_2=5k_a$ und $b-b_2=5k_b$. Nun ist

$$(a+b)-(a_2+b_2)=(a-a_2)+(b-b_2)=5k_a+5k_b$$

durch 5 teilbar. Daher ist $\overline{a+b}=\overline{a_2+b_2}$. □

Auch Subtraktion und Multiplikation ist wohldefiniert (siehe Übung).

Modulo 5 läßt sich auch eine Division als Umkehrung der Multiplikation definieren: Ist also z.B. $\overline{2}\cdot\overline{3}=\overline{1}$, so ist $\overline{1}:\overline{3}=\overline{2}$. Rechnet man jedoch modulo anderer Zahlen, wie z.B. modulo 6, so kommt man dabei in Probleme: Es gilt nämlich $\overline{2}\cdot\overline{3}=\overline{0}$ und $\overline{0}\cdot\overline{3}=\overline{0}$. Was ist jetzt $\overline{0}:\overline{3}$? Die Antwort ist nicht eindeutig. In den Übungen werden wir uns diesem Problem genauer zuwenden.

Gehören a und b der gleichen Klasse modulo p an, so schreibt man auch $a\equiv b \pmod{p}$.

5.b.2 Andere Äquivalenzrelationen

Wir schauen uns nun Vektoren $\binom{x}{y}$ in der Ebene $\mathbb{R}^2$ an und definieren folgende Relation:

Definition 5(12). Für zwei Vektoren $\binom{x_1}{y_1}$ und $\binom{x_2}{y_2}$ definieren wir

$$\begin{pmatrix}x_1\\y_1\end{pmatrix}\sim_r\begin{pmatrix}x_2\\y_2\end{pmatrix},$$

wenn es eine reelle Zahl λ gibt mit

$$\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} = \lambda \cdot \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} \quad \text{(Skalarmultiplikation)}.$$

Ist dies eine Äquivalenzrelation?

- Die *Reflexivität* ist gegeben: Setzen wir $\lambda = 1$, so erhalten wir $\binom{x_1}{y_1} \sim_r \binom{x_1}{y_1}$.
- Die *Symmetrie* ist jedoch verletzt, da für $\lambda = 0$ gilt $\binom{0}{0} = 0 \cdot \binom{1}{1}$, aber umgekehrt $\binom{1}{1} = \lambda \cdot \binom{0}{0}$ nicht erfüllbar ist, da die rechte Seite (egal für welches λ) immer $\binom{0}{0}$ ist.

Wir vermuten das Problem daher bei $\lambda = 0$ und ändern deshalb die Definition wie folgt:

Definition 5(13). Für zwei Vektoren $\binom{x_1}{y_1}$ und $\binom{x_2}{y_2}$ definieren wir

$$\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} \sim_w \begin{pmatrix} x_2 \\ y_2 \end{pmatrix},$$

wenn es eine reelle Zahl $\lambda > 0$ gibt mit

$$\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} = \lambda \cdot \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} \quad \text{(Skalarmultiplikation)}.$$

Bildet dies nun eine Äquivalenzrelation?

- Die *Reflexivität* funktioniert wie oben.
- Die *Symmetrie* ist nun auch gegeben, da aus

  $$\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} = \lambda \cdot \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} \quad \text{folgt, daß} \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} = \frac{1}{\lambda} \begin{pmatrix} x_1 \\ y_1 \end{pmatrix}$$

  ist (Da $\lambda > 0$ ist auch $1/\lambda > 0$).
- Die *Transitivität* läßt sich direkt überprüfen:

  $$\text{Aus} \quad \begin{pmatrix} x_1 \\ y_1 \end{pmatrix} = \lambda \cdot \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} \quad \text{und} \quad \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} = \mu \cdot \begin{pmatrix} x_3 \\ y_3 \end{pmatrix} \quad \text{folgt} \quad \begin{pmatrix} x_1 \\ y_1 \end{pmatrix} = \lambda\mu \cdot \begin{pmatrix} x_3 \\ y_3 \end{pmatrix}$$

Daher haben wir tatsächlich eine Äquivalenzrelation definiert. Die dadurch entstehenden Äquivalenzklassen nennen wir $\overline{\binom{x}{y}}$.

Geometrisch erhalten wir folgendes Bild: Die Äquivalenzklassen sind die von der Null ausgehenden Strahlen (jeweils ohne den Punkt $\binom{0}{0}$ selbst); außerdem bildet der Punkt $\binom{0}{0}$ eine eigene, ein-elementige Äquivalenzklasse.

Nun kann ich z.B. folgendes definieren:

Definition 5(14). Der *Winkel* zwischen zwei Klassen $\overline{\binom{x_1}{y_1}}$ und $\overline{\binom{x_2}{y_2}}$, die jeweils nicht die Null-Klasse sind, ist definiert als der Winkel (gegen den Uhrzeigersinn gemessen) der Vektoren $\binom{x_1}{y_1}$ und $\binom{x_2}{y_2}$.

Man kann leicht überprüfen, daß dies *wohldefiniert* ist; die Länge eines Vektors hat keinen Einfluß auf den Winkel.

6 Mathematischer Formalismus: ∀, ∃ etc.

Satz 6(1). Ein Brötchen ist besser als ewige Glückseligkeit.

Beweis. Folgende Aussagen sind trivialerweise wahr:

- Nichts ist besser als ewige Glückseligkeit.
- Ein Brötchen ist besser als nichts.

Setzt man dies zusammen, ergibt sich: Ein Brötchen ist besser als ewige Glückseligkeit. □

Obiger „Satz" legt nahe, daß es sinnvoll ist, Mathematik auf einem genügend formalisierten Level zu betreiben. Darum soll es in diesem Abschnitt gehen.

6.a Mengen

Wir haben schon häufig mit Mengen zu tun gehabt: Die Menge der natürlichen Zahlen, die Menge der geraden Zahlen, die Menge {Hund, Katze, Maus}. Der Begriff *Menge* ist ein Grundbegriff, der im eigentlichen Sinne nicht definiert werden kann. Man kann nur definieren, welche Operationen auf Mengen zulässig sind, und wie diese vonstatten gehen.

Eine Menge hat *Elemente*: Diese können von beliebiger Gestalt sein, insbesondere auch selbst wieder Mengen. Endliche Mengen gibt man häufig an, indem man ihre Elemente zwischen geschweiften Klammern auflistet, wie z.B. $M =$

$\{1, 2, \{4,5\}\}$; M hat hier genau 3 Elemente, nämlich 1, 2, und $\{4,5\}$. Ist a Element von M, so schreibt man $a \in M$.

Mengen haben *Teilmengen*. Es gilt M ist Teilmenge von N, in Zeichen $M \subset N$, wenn aus $a \in M$ immer folgt, daß $a \in N$. Beispielsweise gilt:

- $\{1,3\} \subset \{1,2,3\}$,
- $\{1,3\} \subset \mathbb{Z}$.

Man kann Teilmengen jedoch auch über eine Eigenschaft angeben, in der Form

$$\{a \in N \mid a \text{ erfüllt Eigenschaft } E\}.$$

E muß dabei eine mathematisch definierte Eigenschaft sein, die von jedem Element entweder erfüllt wird oder nicht (d.h. jedoch nicht, daß wir in der Lage sein müssen, dies auch bei jedem Element vernünftig ausrechnen zu können). Beispiele:

- $\{n \in \mathbb{N} \mid n \text{ ist gerade}\}$
- $\left\{ n \in \mathbb{N} \,\middle|\, n \text{ ist größer als } 2^{1000} \right\}$
- $\{n \in \mathbb{N} \mid n \text{ ist kleiner als } -1\}$

Die letzte Menge ist dabei die sogenannte *leere Menge*. Dies ist die Menge, die überhaupt keine Elemente hat.

Es gibt aber noch weitere Möglichkeiten, aus Mengen neue Mengen zu kreieren:

- Die *Vereinigung* zweier Mengen M und N, in Zeichen $M \cup N$, besteht aus allen Elementen, die in mindestens einer der Mengen enthalten sind.
- Der *Durchschnitt* zweier Mengen M und N, in Zeichen $M \cap N$ besteht aus allen Elementen, die in beiden Mengen enthalten sind.

Die Vereinigung oder der Durchschnitt von Mengen können — ähnlich wie bei Summenzeichen — auch durch einen Laufindex gebildet werden, also:

$$\bigcup_{i=1}^{5} \{i^2\} = \{1,4,9,16,25\}$$
$$\bigcup_{i=1}^{\infty} \{i\} = \mathbb{N}.$$

Das Zeichen ∞ wird dabei für „unendlich" gebraucht, d.h. der Index läuft immer weiter und hört nie auf. Ein weiteres wichtiges Konstrukt ist das *Produkt* zweier Mengen, geschrieben als $M \times N$, welches die Menge aller geordneten Paare (m,n) ist mit $m \in M$ und $n \in N$.

Mengen sind kein ganz unproblematischer Begriff, z.B. gibt es nicht die „Menge aller Mengen"; außerdem muß die gleichzeitige Auswahl von Elementen aus unendlich vielen Mengen über das Auswahlaxiom geregelt werden. Da diese Probleme jedoch in Lineare Algebra I und Analysis I nur am Rande auftreten, werden ich sie hier übergehen.

6.b Abbildungen

Um verschiedene Mengen (die nicht zufällig Teilmengen voneinander sind) miteinander zu vergleichen, brauchen wir weitere Hilfsmittel. Grundgerüst hierfür sind die sogenannten *Abbildungen* oder *Funktionen*.

Definition 6(2). Eine Abbildung f von einer Mengen M in eine Menge N (in Zeichen $f : M \to N$) ordnet jedem Element aus M genau ein Element aus N zu. Man schreibt $f(a)$ für das Element in N, welches dem Element $a \in M$ zugeordnet wird.

Abbildungen sind uns in der Schule schon oft begegnet, z.B. als Funktionen von $\mathbb{R} \to \mathbb{R}$ in der Differentialrechnung. Hat eine Menge bestimmte Zusatzstrukturen, wie z.B. $\mathbb{R}$, so kann man von *stetigen* oder *differenzierbaren* Funktionen reden. Dies wird in Analysis I behandelt. Für Abbildungen zwischen beliebigen Mengen M und N sind folgende Eigenschaften besonders relevant:

- Eine Abbildung $f : M \to N$ heißt *injektiv*, falls es für jedes $b \in N$ *höchstens* ein $a \in M$ gibt mit $f(a) = b$.
- Eine Abbildung $f : M \to N$ heißt *surjektiv*, falls es für jedes $b \in N$ *mindestens* ein $a \in M$ gibt mit $f(a) = b$.
- Eine Abbildung $f : M \to N$ heißt *bijektiv*, falls es für jedes $b \in N$ *genau* ein $a \in M$ gibt mit $f(a) = b$.

Surjektivität und Injektivität implizieren zusammen Bijektivität. Ein paar Beispiele:

- Sei $f : \{1,2\} \to \{1,2,3\}$ definiert als $f(x) = x$. Dann ist f injektiv.
- Sei $f : \mathbb{N} \to \{0,1\}$ definiert als $f(x) = 1$, falls x ungerade und $f(x) = 0$, falls x gerade. Dann ist f surjektiv.
- Sei $f : M \to M$ (mit M gleich der Menge der Äquivalenzklassen modulo 5) definiert als $f(\overline{a}) = \overline{a+1}$. Dann ist f bijektiv.

Im letzten Fall muß natürlich überprüft werden, daß f wohldefiniert ist, da es über $\overline{a}$ definiert ist.

Eine Abbildung kann auch mehrere Parameter haben: Eine Abbildung $f : M \times N \to K$ definiert ein Element $f(m,n)$ in K in Abhängigkeit von $m \in M$ und $n \in M$. Beispielsweise ist eine Relation $\sim$ eine Abbildung von $M \times M \to \{\text{ja}, \text{nein}\}$; dabei wird zwei Elementen genau dann „ja" zugewiesen, wenn sie in Relation zueinander stehen.

6.c Aussagenlogik

Verschiedene Aussagen stehen häufig in einer logischen Beziehung zueinander. Betrachtet man zwei mathematische Aussagen A und B, so schreibt man häufig $A \Rightarrow B$ für „aus A folgt B". Dies bedeutet logisch gesehen nicht, daß es eine inhaltliche Beziehung zwischen beiden Aussagen gibt, sondern nur, daß es eine bestimmte Beziehung ihres Wahrheitsgehaltes gibt. Folgende Tabelle beschreibt diese Beziehung:

A	B	$A \Rightarrow B$
wahr	wahr	wahr
wahr	falsch	falsch
falsch	wahr	wahr
falsch	falsch	wahr

Man sieht an dieser Tabelle auch: Wenn $A \Rightarrow B$ gilt und B falsch ist, dann ist A auch falsch. Dies ist das Prinzip, welches dem Beweis durch Widerspruch zugrundeliegt. Beispiele:

$$1 = 1 \Rightarrow \text{ Es gibt unendlich viele Primzahlen}$$
$$1 = 2 \Rightarrow \text{ Es gibt unendlich viele Primzahlen}$$

Gilt $A \Rightarrow B$ und $B \Rightarrow A$, so bezeichnet man dies als $A \Leftrightarrow B$ (Äquivalenz). Beide Aussagen sind dann immer simultan wahr oder falsch.

6.d Existenz- und Allquantor

Häufig will man Aussagen der Form treffen wie:

- Für jedes Element m aus M gilt...
- Für alle Elemente aus M gilt...

Dafür gibt es eine abkürzende Schreibweise: $\forall m \in M$. Beispielsweise gilt $\forall n \in \mathbb{N} : n > -1$.

Desweiteren betrachtet man häufig Aussagen der Form:

- Es gibt ein m in M, so daß ...
- Mindestens ein Element aus M erfüllt ...

Hierfür gibt es auch eine Schreibwiese: $\exists m \in M$. Beispielsweise gilt $\exists n \in \mathbb{N}$: n ist Primzahl.

Beide Schreibweisen hängen eng miteinander zusammen, wie folgende Erläuterung zeigen soll. Sei $A(m)$ eine Aussage, die von einem Element in m abhängt (so etwas wie: m ist eine Primzahl). Dann gilt folgende Äquivalenz:

$$\text{nicht } \big(\forall m \in M : A(m)\big) \iff \exists m \in M : \text{nicht } A(m).$$

In Worten kann man dies folgendermaßen ausdrücken: Wenn etwas nicht für alle Elemente einer Menge M gilt, so gibt es ein Element von M, für das es nicht gilt (und umgekehrt).

Daher lassen sich sich ∀-Aussagen durch ein einziges Gegenbeispiel widerlegen („Alle Primzahlen sind ungerade" wird durch 2 widerlegt). Andersherum können noch so viele Beispiele keine ∀-Aussage beweisen.

Man kann beide Quantoren auch in Abhängigkeit voneinander benutzen. So ist zum Beispiel folgende Aussage korrekt:

$$\forall n \in \mathbb{N} \exists m \in \mathbb{N} : m > n$$

In Worten formuliert: Für jede natürliche Zahl n gibt es eine, die größer ist (z.B. $n+1$).

Wichtig: Existenz- und Allquantoren sind nicht einfach vertauschbar! Betrachten wir dazu obiges Beispiel:

Lemma 6(3). Die Aussage

$$\exists m \in \mathbb{N} \forall n \in \mathbb{N} : m > n$$

ist falsch.

Beweis. Übung. □

7 Axiomatik

Wie definiert man die Menge der natürlichen Zahlen? Ein Informatiker würde darauf vielleicht folgende Antwort geben:

Definition 7(1) (Informatiker)**.** Wir betrachten alle Strings endlicher Länge aus den Elementen 0 und 1, die mit einer 1 beginnen. Wir definieren die Menge der natürlichen Zahlen als Menge dieser Strings. Der Größenvergleich erfolgt über den üblichen Vergleich von Binärzahlen.

Diese Definition ist sinnvoll und auch für gewisse Zwecke brauchbar. Man kann aus ihr herleiten, daß es eine kleinstes natürliche Zahl gibt, daß jede natürliche Zahl genau einen Nachfolger hat und das vollständige Induktion funktioniert.

Doch könnte jemand anderes sagen: Ich möchte die natürlichen Zahlen über Strings aus 0, 1 und 2 definieren und die Regeln des Dreier-Systems beachten. Schnell wird man einwenden: Das ist doch „das Gleiche". Doch was bedeutet dies genau? Wir wollen, daß natürliche Zahlen gewissen Bedingungen genügen, damit wir sie vernünftig benutzen können. Grundprinzip ist dabei das „Abzählen", d.h. das Prinzip, daß natürliche Zahlen an einer Stelle beginnen und man sie „eine nach der anderen" durchlaufen kann. Eine sinnvolle Auflistung von Bedingungen ist etwa die folgende:

1. 1 ist eine natürliche Zahl.
2. Zu jeder natürlichen Zahl n gibt es genau einen Nachfolger n', der ebenfalls eine natürliche Zahl ist.
3. Es gibt keine natürliche Zahl, deren Nachfolger 1 ist.
4. Jede natürliche Zahl ist Nachfolger höchstens einer natürlichen Zahl.
5. Von allen Mengen X, welche
   - die Zahl 1 und
   - mit einer natürlichen Zahl n auch stets deren Nachfolger n' enthalten, ist die Menge der natürlichen Zahlen die kleinste.

Die letzte Bedingung wirkt vielleicht etwas seltsam; man könnte sie klarer und weniger formal definieren als: Vollständige Induktion funktioniert. Denn durch sie ist sichergestellt, daß eine Aussage, die für 1 und für jeden Nachfolger einer natürlichen Zahl gilt, auch für jede natürliche Zahl gilt. Ein Beispiel hierzu werden wir weiter unten sehen.

Wenn wir diese Eigenschaften brauchen (und nur diese, wie sich herausstellt), warum nennen wir dann nicht jede Menge, die sie erfüllt, die natürlichen Zahlen? Genau das werden ab sofort tun.

Wir wollen dies noch einmal ordentlich und formal korrekt tun:

Definition 7(2) (Mathematiker)**.** Gegeben ist eine Menge M, sowie ein Element darin, welches wir $\overline{1}$ nennen (Axiom 1). Weiterhin ist eine Abbildung Nach : $M \to M$ gegeben (Axiom 2). Wir fordern außerdem folgende Bedingungen (die sogenannten *Peano-Axiome*):

3. Es gibt kein $m \in M$ mit $\text{Nach}(m) = \overline{1}$.
4. Nach ist injektiv.
5. Von allen Mengen X, welche
   - das Element $\overline{1}$ und
   - mit einem Element $m \in M$ auch stets $\text{Nach}(m)$ enthalten (in Zeichen $m \in M \cap X \Rightarrow \text{Nach}(m) \in X$), ist die Menge M die kleinste.

Dann nennen wir *M die Menge der natürlichen Zahlen.*

Wie sich leicht überprüfen läßt, stimmen die Axiome 1 bis 5 mit den oben definierten Bedingungen 1 bis 5 überein.

Im Prinzip gibt es nun also verschiedene Mengen M, die man natürliche Zahlen nennen könnte. Betrachten wir z.B. $\mathbb{N} \cup \{0\}$ und definieren $\overline{1}$ als 0, so erfüllt dies auch alle gestellten Bedingungen. Aber müssen wir diese Mengen wirklich unterscheiden? In allen Grundeigenschaften stimmen sie überein; und aus diesen Grundeigenschaften läßt sich alles weitere definieren, wie z.B. Addition, Multiplikation, Primzahlen etc.

Lassen wir jedoch einzelne Axiome weg, so treten Probleme auf. Folgende Menge M erfüllt z.B. die ersten vier Axiome:

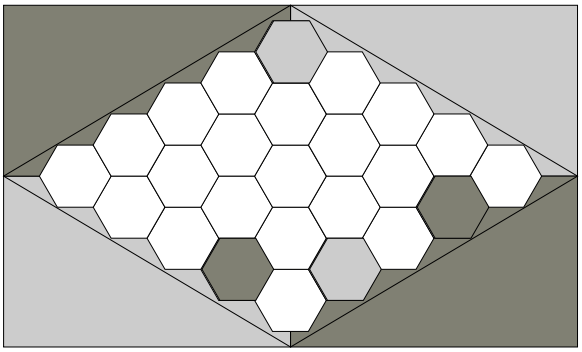
$$M := \{q \in \mathbb{Q} \mid q \geq 1\} \qquad \overline{1} := 1 \qquad \text{Nach}(q) := q + 1$$

Nach ist eine injektive Abbildung, die nie die $\overline{1}$ trifft. Untersuchen wir das fünfte Axiom, so stellen wir fest, daß $X = \mathbb{N}$ den Bedingungen $\overline{1} \in X$ und $m \in M \cap X \Rightarrow \text{Nach}(m) \in X$ genügt, aber kleiner als M ist. Das fünfte Axiom ist also nicht erfüllt; vollständige Induktion ist bei dieser Menge zum Scheitern verurteilt.

Weitere Beispiele dazu gibt es in den Übungen.

8 Existenz vs. Konstruierbarkeit

Manche von Ihnen kennen vielleicht das Spiel HEX. Ein typisches HEX-Brett hat die folgende Form:



Es spielen zwei Spieler HELL und DUNKEL. Die Spieler färben immer abwechselnd ein Feld in ihrer Farbe ein, wobei HELL beginnt. Kann ein Spieler die ihm zugordneten beiden Seiten des Spielfeldes verbinden, so hat er gewonnen. Gelingt dies keinem Spieler, bis das Spielfeld ausgefüllt ist, so ist unentschieden.

Spielt man dieses Spiel auf einem hinreichend großen Spielfeld (11×11 oder 14×14 wird häufig benutzt), so ist keine Gewinnstrategie bekannt; das Spiel ist zu umfangreich, um es mit heutigen Computern durchzurechnen.

Trotzdem lassen sich einige interessante mathematische Aussagen über das Spiel treffen. Zuerst beweisen wir folgendes Lemma:

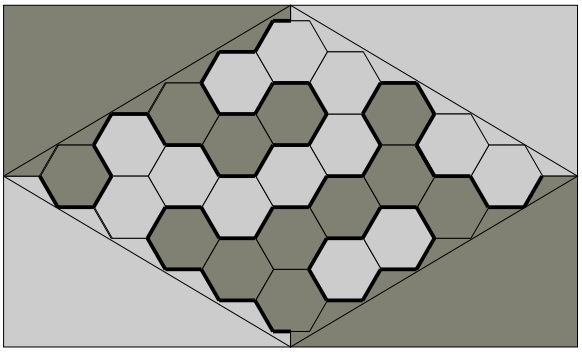
Lemma 8(1). Das Spiel endet nie unentschieden.

Beweis. Wir fassen die Ecken und Kanten der Spielfelder als Graph auf: Wir schauen uns also Pfade entlang von Kanten an, die zwei Eckpunkte verbinden. Zusätzlich zu den sechs Seiten jedes Feldes betrachten wir noch die vier Trennlinien zwischen den Außenbereichen als Kante mit einer Ecke als Ende. Die Außenbereiche werden im Folgenden wie „riesige Felder" der jeweiligen Farbe behandelt.

Unser Graph hat insgesamt vier Enden (also Ecken, von denen nur eine Kante ausgeht). Wir wählen die linke davon als Ausgangspunkt und wollen nun einen Weg durch den Graphen finden, der folgende Bedingung erfüllt: Jede Kante des Weges grenzt an ein helles und an ein dunkles Feld.

Wir wollen nun folgendes beweisen: An jeder Ecke gibt es genau eine Kante, mit der man den Weg fortsetzen kann.

Für die vier Enden ist dies klar. Kommt man ansonsten an eine Ecke, so wird sie von drei Feldern umgeben. Die Kante, von der man kommt, grenzt dabei an ein helles und ein dunkles Feld. Je nachdem, ob das dritte Feld nun hell oder dunkel ist, muß man also nach rechts oder links abbiegen. Wir haben also gezeigt: Es ist immer möglich, den Weg fortzusetzen und diese Fortsetzung ist eindeutig bestimmt. Insgesamt könnte das Bild so aussehen:



Setzen wir den Weg immer weiter fort, so können wir nie zu einer Ecke zurückkehren, an der wir schon waren, da diese Ecke sonst drei Kanten hätte, deren Nachbarfelder verschiedenfarbig sind (was offenbar nicht geht). Der Weg muß daher zwangsweise in einem der anderen drei Enden aufhören (da er überall sonst fortsetzbar ist).

Egal in welchem der drei Enden der Weg aufhört, er verbindet immer zwei gegenüberliegende Ränder des Spielfeldes, also entweder die beiden hellen oder die beiden dunklen (Durch eine kleine Zusatzüberlegung kann man sich überlegen, daß auch das diametral gegenüberliegende Ende des Spielfeldes nicht das Ende des Weges sein kann; dies ist hier aber nicht so entscheidend). Nehmen wir ohne Beschränkung der Allgemeinheit (d.h. der andere Fall ist genauso) an, er verbindet die beiden hellen Ränder des Spielfeldes. Dann wissen wir, daß an unserem Weg an jede Kante ein helles Feld grenzt: Diese bilden also einen verbundenen Weg von Feldern, der möglicherweise mehrmals zum selben Rand zurückkehrt, aber irgendwann beide hellen Ränder miteinander verbindet, da der Weg im Graphen zusammenhängt und beide Ränder berührt. Damit haben wir unseren Weg aus Feldern für den Spieler HELL gefunden. □

Unter einer *Gewinnstrategie* verstehen wir einen Katalog, der dem Spieler abhängig vom aktuellen Spielstand (d.h. seinen bisherigen Zügen und denen des Gegners) nach jedem Zug des Gegners einen weiteren gültigen Zug angibt, so daß der Spieler (wenn er dem Katalog folgt) am Ende gewinnt. Man könnte dies auch als ein Computerprogramm auffassen, welches unfehlbar spielt und immer gewinnt.

Satz 8(2). Auf jedem $n \times n$-HEX-Brett hat HELL eine Gewinnstrategie.

Beweis. Da das Spiel HEX rein deterministisch ist (d.h. nicht von zufälligen Elementen wie Würfeln etc. abhängt), muß, wenn beide Spieler optimal spielen, immer ein bestimmter Spieler gewinnen. Dieser hat damit eine Gewinnstrategie.

Nehmen wir nun an, DUNKEL hätte eine Gewinnstrategie und zeigen damit, daß dann auch HELL eine solche bekommen könnte, indem er die Strategie von

DUNKEL „stiehlt". Da HELL beginnt, stehen in dem Katalog K von DUNKEL nun alle Spielstände aufgelistet, in denen HELL ein Feld mehr hat als DUNKEL (und dazu natürlich der dazu passende optimale Antwortzug).

HELL bräuchte nun einen Katalog, in dem die besten Antworten auf alle Spielstände stehen, bei denen HELL und DUNKEL gleich viele Felder belegt haben. Um nun trotzdem den Katalog von DUNKEL benutzen zu können, bedient er sich folgenden Prinzips: Ein Zug kann für einen Spieler nie von Nachteil sein; ein Feld in der eigenen Farbe ist immer mindestens so gut wie ein leeres Feld. Er kann also den Katalog von DUNKEL mit umgedrehten Farben benutzen, wenn er zusätzlich ein beliebiges freies Feld als dunkel annimmt.

Formal gehen wir wie folgt vor: Wir numerieren die Felder von 1 bis n^2. HELL erstellt nun seinen eigenen Katalog auf folgende Weise: Er vertauscht in dem Katalog von DUNKEL die Farben. Diesen neuen Katalog nennen wir K^{-1}. Er listet nun alle Spielstände auf, die ein dunkles Feld mehr haben. Der Katalog K_{HELL} von HELL findet nun auf alle Spielstände mit gleich vielen hellen und dunklen Feldern wie folgt eine Antwort:

1. Bestimme das weiße Feld mit der kleinsten Nummer.
2. Nehme für Schritt 3 an, dieses Feld wäre dunkel.
3. Schaue den so entstandenen Spielstand in K^{-1} nach.

Da K den Spieler DUNKEL zum Sieg führt, muß auch K_{HELL} den Spieler HELL zu Sieg führen. Es können jedoch nicht beide Spieler eine Gewinnstrategie haben: Wir haben einen Widerspruch. Damit ist die Existenz einer Gewinnstrategie für DUNKEL unmöglich. Daher muß HELL eine solche haben. □

Der obenstehende Satz beweist also mathematisch einwandfrei, daß HELL bei optimaler Spielweise immer gewinnt. Diese optimale Spielweise ist jedoch im Allgemeinen unbekannt.

Beweise durch Widerspruch weisen häufig die *Existenz* eines mathematischen Objektes nach, ohne jedoch Anhaltspunkte zu geben, wie dies eigentlich zu konstruieren sei. In der Analysis werden Sie z.B. lernen, daß sich die allermeisten reellen Zahlen jeglicher Konstruktion entziehen; trotzdem muß man an diesen „schemenhaften" Objekten nicht verzweifeln: Die Mathematik liefert uns Methoden, Aussagen über Objekte zu treffen, die wir in ihrer Komplexität niemals voll erfassen können.

9 Komplexe Zahlen

Einer wichtigsten Begriffe der (Linearen) Algebra ist der des *Körpers*. Grob gesprochen handelt es sich dabei um eine Menge, auf der es zwei Verknüpfungen namens *Addition* und *Multiplikation* gibt, die miteinander verträglich sind. Die aus der Schule bekannten Körper sind die *rationalen Zahlen* und die *reellen Zahlen*. Damit es sich bei einer Menge K um einen Körper handelt, müssen folgende Bedingungen (die *Körperaxiome*) erfüllt sein:

1. **Existenz einer 0 und einer 1:** Es gibt zwei Elemente namens 0 und 1, so daß $\forall a \in K : 0 \cdot a = 0$, $\forall a \in K : 1 \cdot a = a$ und $\forall a \in K : a + 0 = a$.
2. **Assoziativität:** Es gilt für alle $a, b, c \in K$: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ und $(a + b) + c = a + (b + c)$.
3. **Kommutativität:** Es gilt für alle $a, b \in K$: $a \cdot b = b \cdot a$ und $a + b = b + a$.
4. **Distributivität:** Es gilt für alle $a, b, c \in K$: $(a + b) \cdot c = a \cdot c + b \cdot c$.
5. **Existenz von Inversen:** Zu jedem Element $a \in K$ gibt es ein Element $(-a)$ mit $a + (-a) = 0$. Zu jedem Element $a \in K$, welches nicht 0 ist, gibt es ein Element a^{-1} mit $a \cdot a^{-1} = 1$.

Der kleinste denkbare Körper besteht dabei nur aus den Zahlen 0 und 1. Die Zahl (-1) muß hier also auch 0 oder 1 sein; $(-1) = 0$ führt zu dem Widerspruch $1 + 0 = 0$, da schon $1 + 0 = 1$ bekannt ist (Existenz der 0). Somit ist $1 = (-1)$ und damit $1 + 1 = 0$. Dieser Körper entspricht dem Rechnen modulo 2. Nicht jede Restklassenmenge modulo n bildet einen Körper (siehe Übungen).

Wir wollen nun einen weiteren Körper definieren, der in der Mathematik sehr wichtig ist: Der Körper $\mathbb{C}$ der komplexen Zahlen. Für diese Definition werden wir davon ausgehen, daß wir $\mathbb{R}$ bereits definiert haben; dies wird dann formal in Analysis I nachgeholt.

Die Idee, komplexe Zahlen einzuführen, entstand aus folgender Fragestellung: Wie handhabt man die Wurzel aus einer negativen Zahl? Schon vor langer Zeit stellte man fest, daß Ausdrücke wie $\sqrt{-7}$ sich zwar nicht im eigentlichen Sinne ausrechnen lassen, sich aber als algebraische Objekte vernünftig verhalten. Später entwickelte sich daraus eine formale Definition.

Sei dazu $\mathtt{i}$ eine „Zahl" mit $\mathtt{i}^2 = -1$. Die Menge $\mathbb{C}$ der komplexen Zahlen besteht aus den Zahlenpaaren $a + b\mathtt{i}$, wobei $a, b \in \mathbb{R}$. Diese Paare können wir nun Addieren und Multiplizieren:

$$(a + b\mathtt{i}) + (c + d\mathtt{i}) = (a + c) + (b + d)\mathtt{i}$$
$$(a + b\mathtt{i}) \cdot (c + d\mathtt{i}) = ac + ad\mathtt{i} + bc\mathtt{i} + bd\mathtt{i}^2 = (ac - bd) + (ad + bc)\mathtt{i}$$

Um zu sehen, daß die komplexen Zahlen einen Körper bilden, müssen wir die fünf Körperaxiome überprüfen:

1. Die 0 ist gegeben als $0+0\mathtt{i}$ und die 1 als $1+0\mathtt{i}$. Diese erfüllen offenbar die Bedingungen.

2. Folgt aus der Assoziativität der reellen Zahlen.

3. Folgt auch aus der Kommutativität der reellen Zahlen.

4. s.o.

5. Das additive Inverse von $(a+b\mathtt{i})$ ist $(-a-b\mathtt{i})$. Das multiplikative Inverse ist etwas komplizierter zu bestimmen. Löst man die Gleichung $(a+b\mathtt{i})(c+d\mathtt{i})=1$ auf, so erhält man das Gleichungssystem

$$ac-bd=1$$
$$ad+bc=0$$

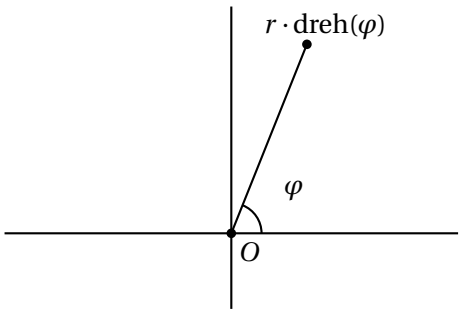
Die Lösungen sind (wie man leicht sieht): $c=a/(a^2+b^2)$, $d=-b/(a^2+b^2)$. Diese sind genau dann definiert, wenn a^2+b^2 nicht Null ist, also wenn gilt $a+b\mathtt{i}\neq 0+0\mathtt{i}$.

Ein wichtiges Resultat über komplexe Zahlen ist:

Lemma 9(1). Zu jeder Zahl $\alpha\in\mathbb{C}$ mit $\alpha\neq 0$ gibt es genau zwei Zahlen $\beta\in\mathbb{C}$ mit $\beta^2=\alpha$. Anders gesagt: Jede nichtverschwindende komplexe Zahl hat genau zwei Wurzeln. Wir nennen eine solche Zahl β eine *verallgemeinerte Quadratwurzel*.

Bevor wir dieses Lemma beweisen, wollen wir uns noch einer anderen Interpretation der komplexen Zahlen zuwenden.

Wie wir gesehen haben, besteht jede komplexe Zahl aus einem Paar (a,b) von reellen Zahlen; wir können eine solche Zahl also auch als Punkte der Ebene auffassen. Punkte in der Ebene können wir aber auch durch sogenannte *Polarkoordinaten* beschreiben: Dabei ordnen wir einem Punkt jeweils einen Abstand r zum Nullpunkt und seinen Winkel φ zu einer vorgegebenen Achse (z.B. der x-Achse) zu.



Der Winkel wird hierbei üblicherweise das Bogenmaß des Winkels ($\pi/2 = 90°$) benutzt. Wir schreiben $a + b\mathtt{i} = r \cdot \mathrm{dreh}(\varphi)$. Dabei ist dreh definiert als $\cos\varphi + \mathtt{i}\sin\varphi$. Aus der Definition von Sinus und Kosinus sieht man sofort, daß $a = r \cdot \cos\varphi$ und $b = r \cdot \sin\varphi$ sein muß (Katheten eines rechtwinkligen Dreiecks).

Was ist nun der Vorteil dieser Sichtweise? Betrachten wir zwei komplexe Zahlen $r_1 \cdot \mathrm{dreh}(\varphi_1)$ und $r_2 \cdot \mathrm{dreh}(\varphi_2)$, so ist ihr Produkt $r_1 r_2 \cdot \mathrm{dreh}(\varphi_1 + \varphi_2)$. Dies läßt sich nachrechnen (Übung). Beispiele für Umrechnungen:

- $1 = 1 \cdot \mathrm{dreh}(0)$
- $\mathtt{i} = 1 \cdot \mathrm{dreh}(\pi/2)$
- $1 + \mathtt{i} = \sqrt{2} \cdot \mathrm{dreh}(\pi/4)$

Statt $\mathrm{dreh}(\varphi)$ schreibt man üblicherweise $\exp(\varphi\mathtt{i})$; da ich aber hier nicht erklären möchte, wie sich die Exponentialfunktion auf die komplexen Zahlen auswirkt, behalte ich die einfachere Schreibweise dreh bei.

Beweis von 9(1). Sei $a + b\mathtt{i} = r \cdot \mathrm{dreh}(\varphi)$ gegeben. Ist $a + b\mathtt{i}$ nicht Null, so ist r positiv und wir können zwei neue Zahlen bilden:

$$\beta_1 = \sqrt{r} \cdot \mathrm{dreh}(\varphi/2)$$
$$\beta_2 = \sqrt{r} \cdot \mathrm{dreh}(\varphi/2 + \pi)$$

Nach obiger Multiplikationsregel ist klar, daß $\beta_1^2 = \beta_2^2 = \alpha$.

Wäre für eine weitere Zahl $r_1 \cdot \mathrm{dreh}(\varphi_1)$ die Gleichung

$$r_1^2 \cdot \mathrm{dreh}(2\varphi_1) = r \cdot \mathrm{dreh}(\varphi)$$

erfüllt, so folgt $r_1 = \sqrt{r}$ und $2\varphi_1 - \varphi$ ist ein Vielfaches von 2π, da die Darstellung einer Zahl als $r \cdot \mathrm{dreh}(\varphi)$ eindeutig ist. Daraus lassen sich genau die obigen beiden Lösungen ableiten. □

Eine sehr wichtige Aussage über komplexe Zahlen, die wir an dieser Stelle nicht beweisen werden, ist:

Satz 9(2) (Fundamentalsatz der Algebra)**.** Jedes Polynom vom Grad n hat genau n (nicht notwendigerweise verschiedene) Nullstellen.

Für Polynome zweiten Grades sieht man dies daran, daß sich die pq-Formel immer ausrechnen läßt.

10 Konstruktion mit Zirkel und Lineal

In diesem Kapitel soll es um Konstruktion mit Zirkel und Lineal gehen: Wir betrachten also die Ebene (auch als $\mathbb{R}^2$ bezeichnet) und konstruieren mit Hilfe eines Zirkels und eines Lineals ohne Markierungen aus vorgegebenen Punkten neue Punkte.

In der Unterstufe und Mittelstufe lernt man Konstruktionslösungen zu verschiedenen klassischen Problemen, wie z.B. der Halbierung einer Strecke, der Errichtung einer Senkrechten, der Konstruktion eines Dreiecks zu drei vorgebenene Längen usw.

Diese Methoden waren allesamt schon den alten Griechen bekannt. Sie versuchten weiterhin bestimmte weitere Probleme zu lösen:

- **Die Quadratur des Kreises:** Kann man zu einem gegebenen Kreis ein Quadrat konstruieren, welches den gleichen Flächeninhalt hat?
- **Die Drittelung des Winkels:** Kann man einen beliebigen Winkel konstruktiv in drei gleiche Teile teilen?
- **Die Verdoppelung des Würfels:** Auch wenn es auf den ersten Blick nicht so scheint, so handelt es sich auch hierbei um ein Konstruktionsproblem der Ebene. Es lautet: Kann man aus der Kantenlänge eines Würfels die Kantenlänge des (volumenmäßig) doppelt so großen Würfels konstruieren?

Diese Probleme wurden sehr berühmt, da sich trotz ihrer jederman verständlichen Aufgabenstellung keine Lösung finden wollte (und dies über Jahrtausende!). Erst vor etwa 200 Jahren erkannte man den Grund hierfür: Es gibt solche Konstruktionen nicht!

Diese Erkenntnisse ist allerdings keine innergeometrische: Ein tieferes Verständnis für die Frage „Was ist konstruierbar und was nicht?" ergab sich erst durch die Übersetzung der Problemstellung in die Algebra. Dies wollen wir im nächsten Abschnitt bewältigen.

10.a Welche Zahlen sind konstruierbar?

(Nach einem Artikel der Zeitschrift $\sqrt{\text{WURZEL}}$).

Wir identifizieren die Ebene mit den komplexen Zahlen. Als Anfangspunkte der Konstruktion wählen wir die Punkte 0 und 1 (wir beschränken uns hier auf zwei Anfangspunkte; für mehr Anfangspunkte kann man sehr ähnlich vorgehen). Nun

wollen wir die Teilmenge K von $\mathbb{C}$ der konstruierbaren Punkte bestimmen. Dafür sollten wir erst einmal genau definieren, was wir unter einem *konstruierbaren Punkt* verstehen. Wir führen auch den Begriff der *konstruierbaren Geraden* und des *konstruierbaren Kreises* ein.

Definition 10(1). Eine Gerade g heiße n-konstruierbar ($n \in \mathbb{N}$), falls es n-konstruierbare Punkte $P \neq Q$ mit $P, Q \in g$ gibt.

Ein Kreis k heiße n-konstruierbar, wenn sein Mittelpunkt n-konstruierbar ist, und sein Radius der Abstand zweier n-konstruierbarer verschiedener Punkte ist.

Ein Punkt $P \in \mathbb{C}$ heiße 0-konstruierbar, falls $P \in \{0, 1\}$ ist.

Ein Punkt $P \in \mathbb{C}$ heiße $(n+1)$-konstruierbar, falls er eine der folgenden Bedingungen erfüllt:

1. P ist n-konstruierbar.
2. P ist Schnittpunkt von zwei n-konstruierbaren nichtparallelen Geraden.
3. P ist Schnittpunkt einer n-konstruierbaren Geraden und mit einem n-konstruierbaren Kreis.
4. P ist Schnittpunkt zweier n-konstruierbarer Kreise, deren Mittelpunkt verschieden sind.

Wie man sieht, erfolgt diese Definition induktiv. Nun sei

$$K := \{P \in \mathbb{C} \mid \exists n \in \mathbb{N} : \text{P ist } n\text{-konstruierbar}\}.$$

Wir wollen diese Menge K nun algebraisch charakterisieren. Dafür wollen wir prüfen, welche algebraischen Operationen in K möglich sind.

Lemma 10(2).

Falls $z, z_1, z_2 \in K$, so auch:

(i) $z_1 + z_2$ und $z_1 - z_2$,

(ii) $|z|$, $\mathtt{Re}\, z$, $\mathtt{Im}\, z$ und $\overline{z}$,

(iii) das Produkt $z_1 \cdot z_2$,

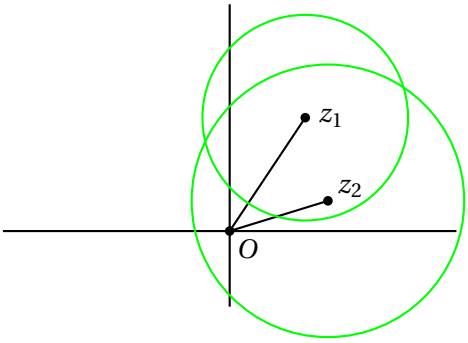
(iv) der Quotient z_1 / z_2, falls $z_2 \neq 0$ und

(v) beide Wurzeln von z, d.h. die beiden Zahlen w_1 und w_2 mit $w_1^2 = w_2^2 = z$.

Dabei bezeichnet $|z|$ den *Betrag* einer komplexen Zahl, also ihren Abstand zum Nullpunkt, $\mathtt{Re}(a + b\mathtt{i}) = a$ und $\mathtt{Im}(a + b\mathtt{i}) = b$ sind der Real- und Imaginärteil und $\overline{a + b\mathtt{i}} = a - b\mathtt{i}$ ist die sogenannte *Konjugation*.

Beweisskizze. Wir verzichten an dieser Stelle darauf, klassische Konstruktionsmethoden und Geometrie der Mittelstufe zu wiederholen.

(i) $z_1 + z_2$ ist ein Schnittpunkt des Kreises um z_1 mit Radius $|z_2|$ mit dem Kreis um z_2 mit Radius $|z_1|$.



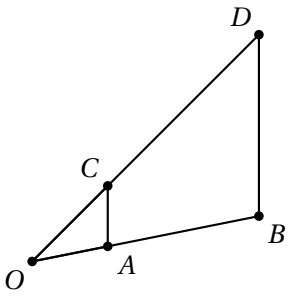
Der Punkt $-z_2$ läßt sich konstruieren, indem man man den Kreis mit Radius $|z_2|$ um 0 mit der Geraden durch z_2 und 0 schneidet. Dann kann man z_1 und $-z_2$ addieren, um $z_1 - z_2$ zu erhalten.

(ii) Zuerst konstruiert man aus den Anfangspunkten die x- und y-Achse. Der Rest ergibt sich leicht durch Projektionen und Spiegelungen.

(iii) Im Strahlensatz betrachtet man vier Längen a_1, a_2, b_1, b_2, für die Gleichung

$$\frac{a_1}{a_2} = \frac{b_1}{b_2}$$

gilt.



Setzen wir hier $a_2 = 1$, so gilt $b_1 = b_2 \cdot a_1$. Auf diese Weise läßt sich eine Multiplikation positiver reeller Zahlen ausführen. Da die Formel für die Multiplikation zweier komplexer Zahlen $a+b\mathtt{i}$ und $c+d\mathtt{i}$ nur die Multiplikation, Subtraktion und Addition reeller Zahlen benutzt, kann auch diese Operation ausgeführt werden.

(iv) Ähnlich wie (iii).

(v) Wie wir bei obigem Lemma über die Existenz der verallgemeinerten Quadratwurzeln gesehen haben, reicht es hier, die Quadratwurzel aus dem Betrag zu ziehen und den Winkel zu halbieren. Die Quadratwurzel aus einer Zahl r kann man z.B. ziehen, indem man den Höhensatz($h^2 = pq$) im rechtwinkligen Dreieck benutzt und $p = 1$ und $q = r$ setzt. Die Halbierung eines Winkels ist eine klassische Konstruktion.

□

Mit Hilfe von Punkt (i) können wir aus der Zahl 1 alle ganzen Zahlen erzeugen. Aus (iii) und (iv) ergibt sich dann, daß sich auf diese Weise alle rationalen Zahlen erzeugen lassen.

Definition 10(3). Eine komplexe Zahl, die sich durch iteriertes Anwenden der Grundrechenarten und ziehen von verallgemeinerten Quadratwurzeln aus einer rationalen Zahl erzeugen läßt, heiße *Surd*. Mit S bezeichnen wir die Menge aller Surds.

Ein Beispiel für ein Surd wäre

$$\sqrt{3+\mathtt{i}\sqrt{2+\frac{\mathtt{i}}{2}}+1},$$

wobei $\sqrt{\alpha}$ eine verallgemeinerte (also nicht eindeutig bestimmte) Quadratwurzel ist. Nach Lemma 10(2) wissen wir folgendes:

Lemma 10(4). Jeder Surd ist konstruierbar.

Wir wollen nun die Umkehrung beweisen. Genauer:

Satz 10(5) (Struktursatz über konstruierbare Zahlen)**.** Sei $z \in \mathbb{C}$. Dann sind folgende Aussagen äquivalent:

(i) $z \in K$.

(ii) $\mathtt{Re}\, z \in S$ und $\mathtt{Im}\, z \in S$.

(iii) $z \in S$.

Beweis. Die Folgerung (ii) ⇒ (iii) ist klar. (iii) ⇒ (i) haben wir gerade gezeigt. Somit bleibt nur noch (i) ⇒ (ii).

Da die Definition von Konstruierbarkeit induktiv erfolgte, bietet es sich an, auch den Beweis dieses Satzes induktiv zu führen. Die zu beweisende Aussage $A(n)$ lautet dann: Ist z eine n-konstruierbare Zahl, so sind $\mathtt{Re}\, z$ und $\mathtt{Im}\, z$ Surds.

Induktionsanfang: Die einzigen 0-konstruierbaren Zahlen sind 0 und 1. Für diese ist die Bedingung erfüllt.

Induktionsschritt: Seien $A(0), \ldots, A(n)$ gezeigt. Dann wollen wir $A(n+1)$ zeigen.

Nach der Definition wissen wir, daß $(n+1)$-konstruierbare Punkte P auf vier verschiedene Weisen aus n-konstruierbaren geometrischen Objekten entstehen können:

1. *P ist n-konstruierbar.* Dann sind wir nach Induktionsvoraussetzung fertig.
2. *P ist Schnittpunkt zweier n-konstruierbarer Geraden.* Zwei n-konstruierbare Geraden sind durch insgesamt vier n-konstruierbare Punkte gegeben. Da diese vier Punkte durch Surds gegeben sind und zur Bestimmung des Schnittpunktes nur ein lineares Gleichungssystem gelöst werden muß, ist auch P wieder durch ein Surd gegeben.
3. *P ist Schnittpunkt einer n-konstruierbaren Gerade mit einem n-konstruierbaren Kreis.* Beide geometrische Objekte sind jeweils durch zwei n-konstruierbare Punkte geben. Die Schnittformel involviert nur Grundrechenarten und Quadratwurzeln.
4. *P ist Schnittpunkt zweier n-konstruierbarer Kreise.* Wie Fall 3.

Damit ist $A(n+1)$ gezeigt. Aus der Induktion folgt (ii). □

Diese Charakterisierung der Menge K wird im nächsten Abschnitt benutzt.

10.b Die Nichkonstruierbarkeit bestimmter klassischer Probleme

10.b.1 Quadratische Körpererweiterungen

Wir betrachten im Folgenden Körper F, die Teilmengen von $\mathbb{C}$ sind. F erbt dabei die Addition und Multiplikation von $\mathbb{C}$, also auch die Kommutativität, Assoziativität etc. Man kann F daher charakterisieren als Untermenge von $\mathbb{C}$, so daß für $z_1, z_2 \in F$ auch $z_1 + z_2$, $z_1 - z_2$, $z_1 \cdot z_2$ und z_1 / z_2 $(z_2 \neq 0)$ in F enthalten sind. Beispiele für solche Körper wären $\mathbb{Q}$ oder $\mathbb{R}$.

Definition 10(6). Sei $F \subset \mathbb{C}$ ein Körper und $\omega \in \mathbb{C} \setminus F$ ($\mathbb{C}$ ohne F) mit $\omega^2 \in F$. Dann sei

$$F(\omega) := \{a + b\omega \mid a, b \in F\}.$$

$F(\omega)$ heißt dann *quadratische Körpererweiterung* zu F.

Beispiele wären:

- Für $F = \mathbb{R}$ und $\omega = \mathtt{i}$ gilt $\mathbb{R}(\mathtt{i}) = \mathbb{C}$.
- Für $F = \mathbb{Q}$ und $\omega = \sqrt{2}$ erhält man Zahlen der Form $a + b\sqrt{2}$.

Für quadratische Körpererweiterungen gilt folgendes Lemma:

Lemma 10(7). (i) Es gilt $a + b\omega = 0$ genau dann wenn $a = b = 0$ $(a, b \in F)$.

(ii) Die Menge $F(\omega)$ ist ein Körper.

Beweis. (i) Ist $b = 0$, so zwingend auch $a = 0$. Ist b jedoch ungleich Null, so folgt aus $a + b\omega = 0$, daß $\omega = -a/b \in F$, was ein Widerspruch ist. Daher folgt aus $a + b\omega = 0$, daß auch $a = b = 0$. Die Umkehrung ist trivial.

(ii) Hier geht man genauso vor wie bei der Erweiterung von $\mathbb{R}$ durch $\mathtt{i}$ zu $\mathbb{R}(\mathtt{i}) = \mathbb{C}$, wobei ω die Rolle von $\mathtt{i}$ einnimmt. Auf diese Weise erhält man Formeln für die Addition, Subtraktion, Multiplikation und Division in $F(\omega)$, die zeigen, daß $F(\omega)$ unter diesen Operationen abgeschlossen ist.

□

Aufgrund von (i) läßt sich eine zahl aus $F(\omega)$ immer auf genau eine Weise als $a + b\omega$ schreiben.

Auch für quadratische Körpererweiterungen läßt sich eine Art Konjugation definieren.

Definition 10(8). Es sei

$$(a + b\omega)^* := a - b\omega \quad (a, b \in F)$$

Für diese Operation gelten die folgenden zwei Lemmata:

Lemma 10(9). Die *-Konjugation verträgt sich mit Addition und Multiplikation. Es gilt:

$$(z_1 + z_2)^* = z_1^* + z_2^* \qquad \text{und} \qquad (z_1 z_2)^* = z_1^* z_2^*$$

Für $z \in F$ gilt $z^* = z$.

Beweis. Schreibt man $z_1 = (a_1 + b_1\omega)$ und $z_2 = (a_2 + b_2\omega)$, so läßt sich dies durch Klammernauflösen einfach nachrechnen. □

Lemma 10(10). Ist P ein Polynom mit rationalen Koeffizienten, so gilt

$$P(z)^* = P(z^*)$$

für alle $z \in F(\omega)$.

Beweis. Die Menge $\mathbb{Q}$ ist in jedem Unterkörper $F \subset \mathbb{C}$ enthalten, da sie durch Grundrechenarten aus $0,1$ erzeugt werden kann und 0 und 1 in jedem Körper enthalten sind. Für alle Elemente $c \in \mathbb{Q}$ gilt daher: $c = c^*$, wie gerade gezeigt. Durch sukzessives Anwenden von Lemma 10(9) erhalten wir:

$$\begin{aligned} P(z)^* &= (a_n z^n + \ldots + a_0 z^0)^* = a_n^* (z^n)^* + \ldots + a_0^* (z^0)^* \\ &= a_n (z^*)^n + \ldots + a_0 (z^*)^0 = P(z^*). \end{aligned}$$

□

10.b.2 Gleichungen dritten Grades

Der folgende Satz bildet die Grundlage für unsere Nichtkonstruierbarkeitsbeweise:

Satz 10(11). Seien $p, q, r \in \mathbb{Q}$. Besitzt das kubische Polynom

$$P(z) = z^3 + pz^2 + qz + r$$

keine rationale Nullstelle, so ist keine der Nullstellen ein Surd.

Beweis. Surds entstehen durch Grundrechenarten und endlich vielem (verallgemeinertem) Quadratwurzelziehen aus einer rationalen Zahl. Daher gibt es zu einem Surd z eine endliche Folge

$$\mathbb{Q} = F_0 \subset F_1 \subset \ldots \subset F_n$$

von quadratischen Körpererweiterungen, so daß $z \in F_n$.

Wir nehmen das Gegenteil der Aussage des Satzes an: Es gibt keine rationalen Nullstellen, doch ist eine der Nullstellen ein Surd. Sei z_1 das Nullstellen-Surd, für das die Folge $F_0 \subset \ldots \subset F_n$ am kürzesten ist. Da z_1 nicht rational ist, muß hierbei $n \geq 1$ sein.

Sei nun $\omega \in F_n$ mit $F_n = F_{n-1}(\omega)$. Dann läßt sich z_1 darstellen als $a + b\omega$ mit $b \neq 0$ (sonst wäre z_1 schon in F_{n-1}). Sei $z_2 := z_1^* = a - b\omega$. Dann ist auch z_2 eine Nullstelle von P, denn

$$P(z_2) = P(z_1^*) = P(z_1)^* = 0^* = 0.$$

Offenbar ist $z_1 \neq z_2$, denn $z_1 - z_2 = 2b\omega \neq 0$. Ist z_3 die dritte Nullstelle, so können wir $P(z)$ wie folgt faktorisieren:

$$\begin{aligned} P(z) &= (z - z_1)(z - z_2)(z - z_3) \\ &= z^3 - (z_1 + z_2 + z_3)z^2 + (z_2 z_3 + z_1 z_3 + z_1 z_2)z - z_1 z_2 z_3. \end{aligned}$$

Der Vergleich der Koeffizienten ergibt:

$$p = -z_1 - z_2 - z_3$$
$$z_3 = -z_1 - z_2 - p = -(a+b\omega) - (a-b\omega) - p = -2a - p \in F_{n-1}.$$

Wir haben also eine Nullstelle in F_{n-1} gefunden, was unserer Annahme über die Minimalität von n widerspricht. Somit kann eine Nullstelle nur ein Surd sein, wenn es mindestens eine rationale Nullstelle gibt. □

Hat ein kubisches Polynom mit rationalen Koeffizienten also keine rationale Nullstelle, so ist nach Satz auch keine Nullstelle konstruierbar. Auf diese Weise haben wir ein Tool in der Hand, mit dem wir zeigen können, daß eine Zahl nicht konstruierbar ist.

Korollar 10(12). Die Würfelverdoppelung ist mir Zirkel und Lineal nicht möglich.

Beweis. Für die Würfelverdoppelung ist es nötig, aus der Länge 1 die Länge $\sqrt[3]{2}$ zu konstruieren. Diese Zahl ist Nullstelle des Polynoms $z^3 - 2$. Die Nullstellen dieses Polynoms sind $\sqrt[3]{2}$, $\sqrt[3]{2}\cdot(\cos 2\pi/3 + \mathtt{i}\sin 2\pi/3)$ und $\sqrt[3]{2}\cdot(\cos 4\pi/3 + \mathtt{i}\sin 4\pi/3)$ (Dies kann man theoretisch herleiten oder nachrechnen). Alle diese Nullstellen sind nicht rational, daher kann nach Satz 10(11) auch keine der Nullstellen konstruierbar sein. Dies beweist die Aussage. □

Häufig kann man alle rationalen Nullstellen eines Polynoms mit folgender Methode finden:

Lemma 10(13). Seien p, q und r *ganze* Zahlen. Dann ist jede rationale Nullstelle von

$$P(z) = z^3 + pz^2 + qz + r$$

eine ganze Zahl, die r teilt.

Beweis. Sei $z_0 = k/l$ eine rationale Nullstelle von $P(z)$ mit teilerfremden Zahlen k, l und $l > 0$. Dann gilt:

$$\frac{k^3}{l^3} + p\cdot\frac{k^2}{l^2} + q\cdot\frac{k}{l} + r = 0$$
$$k^3 + pk^2l + qkl^2 + rl^3 = 0$$

Da alle anderen Zahlen durch l teilbar sind, muß auch k^3 durch l teilbar sein. Damit folgt aber $l = 1$, da k und l teilerfremd sind. Somit gilt:

$$k^3 + pk^2 + qk + r = 0$$

Damit ist aber r durch k teilbar. □

Korollar 10(14). Man kann nicht jeden (konstruierbaren) Winkel mit Zirkel und Lineal dritteln.

Beweis. Wir betrachten einen 120°-Winkel. Dieser läßt sich z.B. durch Zusammensetzung zweier gleichseitiger Dreiecke konstruieren.

Könnte man diesen Winkel dritteln, so ließe sich ein 40°-Winkel konstruieren. Konstruiert man rechtwinkliges Dreieck, welches 40° als einen seiner Winkel hat, so folgt, daß sich $\cos 40°$ konstruieren ließe. Dies wollen wir nun widerlegen.

Mit Hilfe der Additionstheoreme für Sinus und Kosinus läßt sich zeigen (was wir hier nicht vorrechnen wollen):

$$\cos 3\varphi = 4\cos^3\varphi - 3\cos\varphi.$$

Eine formale Definition von Sinus und Kosinus, sowie der Additionstheoreme vertage ich auf Analysis I. Eine elementare Einführung dazu findet sich in jedem Mathe-Buch der 10. Klasse.

Setzt man hier $\varphi = 40°$, so ergibt sich

$$-\frac{1}{2} = \cos 120° = 4\cos^3 40° - 3\cos 40° = \frac{1}{2}z_1^3 - \frac{3}{2}z_1$$
$$z_1^3 - 3z_1 + 1 = 0$$

für $z_1 = 2\cos 40°$. Nach dem Lemma kann eine rationale Nullstelle von $z^3 - 3z + 1$ nur 1 oder -1 sein. Da diese beiden Zahlen jedoch keine Nullstellen sind, wie man leicht überprüft, kann die Nullstelle $z_1 = 2\cos 40°$ keine konstruierbare Zahl sein. □

10.b.3 Die Quadratur des Kreises (ohne Beweis)

Da ein Kreis mit Radius 1 die Fläche π hat, müßte man hierfür ein Quadrat mit Seitenlänge $\sqrt{\pi}$ konstruieren.

Dieses Problem läßt sich leider nicht mit dem Satz über kubische Polynome lösen, da es kein Polynom gibt, welches π (oder $\sqrt{\pi}$) als Nullstelle hat. Diese Eigenschaft nennt man *Transzendenz*. Dies können wir an dieser Stelle nicht beweisen. Wir wollen aber einen kurzen Abriß darüber geben, wie sich dieses Ergebnis entwickelt hat.

Bereits in der Antike interessierten sich die Menschen aus rein praktischen Gründen für Näherungen von π. Schon vor ca. 4000 Jahren hatten die Babylonier eine Konstruktion, die auf die Näherung $\pi \approx 3\frac{1}{8}$ schließen läßt, auf einer Keilschrifttafel hinterlassen.

Der erste, der sich ernsthaft zur Aufgabe gemacht hat, den Kreis exakt zu quadrieren, war wohl der Grieche ANAXAGORAS (500-428 v.Chr.). Er wurde in Athen

wegen Gottlosigkeit ins Gefängnis geworfen, da er behauptete, daß der Mond lediglich das Sonnenlicht reflektiere, und so die göttliche Natur der Sonne in Zweifel zog. Eingekerkert beschäftigte sich ANAXAGORAS dann intensiv mit der Quadratur des Kreises. Darauf wurde dieses Problem sehr populär und verbreitete sich schnell. Schon ARISTOPHANES (ca. 445-386 v.Chr.) verspottete die Kreisquadrierer. Die Griechen erfanden sogar ein eigenes Wort für „sich mit der Quadratur des Kreises beschäftigen". Bemerkenswerterweise sind von den Griechen keine falschen Beweise überliefert, die die Quadratur des Kreises beweisen sollten. Leider sind spätere Amateur-Mathematiker nicht diesem Beispiel gefolgt und behaupteten fälschlicherweise mit eiserner Standhaftigkeit, eine unumstößliche Zirkel-und-Lineal-Konstruktion gefunden zu haben.

Durch Einkästelung des Kreises durch n-Ecke (mit n groß) läßt sich π prinzipiell beliebig genau approximieren. Dies blieb bis zum 15. Jahrhundert die einzige Methode, π anzunähern. Der Mathematik-Professor LUDOLPH VAN CEULEN (ca. 1539-1610) baute ebenfalls auf die Idee von ARCHIMEDES auf und errechnete anhand eines regelmäßigen $(60 \cdot 2^{33})$-Ecks 20 Dezimalen von π, mehr als alle seine Vorgänger. Kurz bevor er starb, gab er sogar 34 Stellen von π an und bat darum, diese auf seinen Grabstein zu meißeln.

Zur Zeit der Analysis kam endlich wieder Bewegung ins Spiel. Man fand etliche Reihen und Produkte, die gegen π konvergieren und gute Näherungsformeln für π liefern. Das hilft zwar, π immer näher zu kommen, aber bringt einen nicht wirklich näher an eien Konstruktion mit Zirkel und Lineal. Einen riesigen Schritt voraus machte LAMBERT im Jahr 1761, indem er zeigte, daß π irrational ist. Leider führte dies zu einer Flut von Amateurbeweisen für die Quadrierung des Kreises, so daß die Paris Académie des Sciences 1775 den folgenden Beschluß faßte:

> Die Akademie hat in diesem Jahr den Beschluß gefaßt, in Zukunft keine Lösungen der Probleme der Verdoppelung des Würfels, der Dreiteilung des Winkels und der Quadratur des Kreies mehr zu überprüfen; ebenso werden auch keine als Perpetuum mobile angekündigten Maschinen mehr überprüft. [...]
>
> Die Menschenfreundlichkeit gebietet es demnach, daß die Akademie, die von der absoluten Nutzlosigkeit der Überprüfung der Kreisquadrierungslösungen überzeugt ist, durch eine öffentliche Erklärung weitverbreitetetn Auffassungen ein Ende setzt, die für mehrere Familien verhängnisvoll gewesen sind [...] Die Quadratur des Kreises ist das einzige der von der Akademie zurückgewiesenenen Probleme, das Anlaß zu einer nützlichen Forschungsarbeit geben könnte. Und wenn ein Geometer diese Quadratur fände, dann würde der Beschluß der Akademie seinen Ruhm nur noch mehren, indem er zeigt, welche Auffassung die Geometer von der Schwierigkeit (um nicht zu sagen: von der Unlösbarkeit) des Problems haben.

Wenige Jahre späte riegelte sich auch die Royal Society in London gegen jegliche „Beweise", welche die Quadratur des Kreises zeigen sollten, ab. DE MORGAN bezeichnete dies 100 Jahre später als den offiziellen Schlag gegen die Kreisquadrierer. Er schlug übrigens sogar vor, die Kreisquadrierer-Krankheit als *morbus cyclometricus* zu bezeichnen. Das kam nicht von ungefähr, denn auch er hatte mit Kreisquadierern zu kämpfen. Beispielsweise war da ein gewisser JAMES SMITH, der in mehreren Büchern versuchte $\pi = 3\frac{1}{8}$ zu beweisen. Daraus konnte er natürlich die Quadratur des Kreises ableiten, aber weder DE MORGAN und HAMILTON noch andere konnten ihn von seinen Fehlern überzeugen.

Der Durchbruch gelang FERDINAND VON LINDEMANN (1852-1939) im Jahr 1882, als er die Transzendenz von π bewies. Damit ist auch gezeigt, daß die Quadratur des Kreises mit Zirkel und Lineal unmöglich ist. Der Beweis würde etwa 6 bis 8 Seiten einnehmen und wird hier nicht geführt.

A Ausblick: Lineare Algebra

Die lineare Algebra studiert Vektorräume ($\mathbb{R}^2$ und $\mathbb{R}^3$ sind aus der Schule bekannt) und Abbildungen zwischen ihnen.

Vektorräume werden dabei abstrakt definiert als Mengen, auf denen es eine Addition und eine Multiplikation mit Skalaren (also Elementen des Grundkörpers) gibt. Am Anfang des Semesters zeigt man zuerst einige wichtige Eigenschaften zu Vektorräumen.

Jeder (endlichdimensionale) Vektorraum V hat eine Basis: Es gibt also Elemente $v_1, \ldots, v_n \in V$, so daß sich alle Elemente des Vektorraums eindeutig darstellen lassen als $\lambda_1 v_1 + \ldots + \lambda_n v_n$, wobei $\lambda_1, \ldots, \lambda_n$ aus dem Grundkörper stammen. Im Fall von $\mathbb{R}^3$ können wir z.B. $v_1 = (1 \quad 0 \quad 0)$, $v_2 = (0 \quad 1 \quad 0)$ und $v_3 = (0 \quad 0 \quad 1)$ wählen; dann gibt es für jeden Vektor $v \in \mathbb{R}^3$ reelle Zahlen $\lambda_1, \lambda_2, \lambda_3$, so daß $v = \lambda_1 v_1 + \lambda_2 v_2 + \lambda_3 v_3$ gilt.

Jeder Vektorraum hat viele verschiedene Basen. Hält man allerdings eine fest, so kann man die linearen Abbildungen zwischen einem Vektorraum V und einem Vektorraum W durch eine Matrix beschreiben. Ein wichtiges Thema ist es, eine „gute" Basis zu finden, in der die Matrix möglichst einfach aussieht. Auf diese Weise lassen sich auch alle linearen Abbildungen klassifizieren (durch die *Jordan-Normalform*).

Wichtig sind auch die *Eigenvektoren*. Hierbei handelt es sich um Vektoren v mit $Mv = \lambda \cdot v$ für eine lineare Abbildung M und eine reelle Zahl λ. Es sind also Vektoren, die durch M auf ein Vielfaches von sich selbst abgebildet werden. Für jede Abbildung M kann dabei λ nur ganz bestimmte Werte annehmen, die sich über die Nullstellen eines Polynoms, des *charakteristischen Polynoms*, bestimmen lassen. Sie sagen viel aus über den „Charakter" der Abbildung.

Ein gutes Buch, welches in etwa den Stoff von Lineare Algebra I und II abdeckt, ist der FISCHER, welcher auch in meinem Semesterapparat steht.

B Ausblick: Analysis

Der erste zentrale Begriff der Analysis ist der des *Grenzwertes*. Man betrachtet Folgen $a_1, a_2, a_3, \ldots$ und stellt Bedingungen auf, wann ein Grenzwert existiert, und wie dieser dann definiert ist.

Ein wichtiger Begriff ist der der *Cauchy-Folge*: Dabei handelt es sich um Folgen, bei denen für große $n, m \in \mathbb{N}$ der Abstand $\| a_n - a_m \|$ beliebig klein wird. Von solchen Folgen möchte man, daß sie gegen eine Zahl konvergieren; in den rationalen Zahlen funktioniert dies jedoch nicht. Diese haben sozusagen „Lücken". Um diese zu stopfen, führt man die *reellen Zahlen* ein. Man sie auf verschiedene Weisen definieren: Eine übliche Definition ist, die über bestimmte Äquivalenzklasse von Cauchy-Folgen zu tun. Man kann die reellen Zahlen auch als unendlich lange Dezimalbrüche auffassen; letztendlich sind alle Sichtweisen äquivalent und haben ihre Vor- und Nachteile.

Hat man Grenzwerte und reelle Zahlen eingeführt, so kann man sich dem Begriff der *Stetigkeit* zuwenden. Dieser läßt sich nun formal definieren. Ein wichtiges Resultat über stetige Funktionen ist der *Zwischenwertsatz*: Eine stetige Funktion, die an einer Stelle positiv und an einer anderen Stelle negativ ist, hat dazwischen einen Wert, an dem sie genau Null ist.

Strenger als der Begriff der Stetigkeit ist der Begriff der *Differenzierbarkeit*. Hier definiert man Ableitungen, und betrachtet auch unendlich lange Polynome, sogenannte *Potenzreihen*. In vielen Fällen läßt sich eine differenzierbare Funktion durch eine Potenzreihe, die *Taylorreihe*, annähern.

Nach der Differenzierbarkeit wendet man sich Integralen zu und definiert diese formal. Bestimmte Methoden, die häufig schon im Mathe-LK behandelt werden, werden bewiesen, erläutert und vertieft.

In Analysis II wendet man sich dann der Differentialrechnung in mehrdimensionalen Räumen zu; hier ergeben sich dann Verbindungen zur Linearen Algebra.

Eine gute Einführung in die Analysis, die etwa das erste Semester abdeckt, ohne zu sehr abzuschweifen, ist das Buch von FORSTER.

C Präsenzübungen

Präsenzübungen sollen in Gruppen von 2 bis 4 Studenten bearbeitet werden. Im Mittel sollte dabei ein Blatt in etwa 45 Minuten bearbeitet werden, wovon natürlich abgewichen werden kann (und manchmal muß).

Präsenzübung 1a

Voraussetzungen: Bis einschließlich Abschnitt 3.

Übung 1. Handelt es sich bei folgenden Zeilen um Definitionen?

1. Sei r eine rationale Zahl. Dann heißt $q = \frac{1}{r}$ das *Inverse* von r.
2. Sei h die erste Nachkommastelle von $\sqrt{2}$ (in ihrer Darstellung als Dezimalzahl).
3. Eine rationale Zahl r heißt *ganze Zahl*, falls es zwei ganze Zahlen p und q gibt mit $r = p/q$ und $q = 1$.

Übung 2 (Beweis oder nicht?)**.**

Satz (I). Die Zahl 15 ist keine Primzahl.

Beweis. Sei t der kleinste Teiler von 15, der größer als 1 ist und s irgendein Teiler. Sei k der größte gemeinsame Teiler von t und s. Dann sind t/k und s/k auch Teiler von 15. Außerdem sind beide zueinander teilerfremd. Damit hat 15 zwei zueinander teilerfremde Teiler und ist damit keine Primzahl. □

Präsenzübung 1b

Voraussetzungen: Bis einschließlich Abschnitt 4.a.

Übung 3 (Beweis oder nicht?)**.**

Satz (II). Der kleinste von 1 verschiedene Teiler einer natürlichen Zahl n ist immer kleiner oder gleich $\sqrt{n}$.

Beweis. Sei t der kleinste Teiler von n, der nicht 1 ist. Dann ist n/t auch ein Teiler von n. Da t jedoch der kleinste ist, gilt: $n/t \geq t$. Form man dies um, so ergibt sich $t \leq \sqrt{n}$, wie gewünscht. □

Übung 4 (Beweis durch Widerspruch)**.**
Beweise: Es gibt keine größte natürliche Zahl.

Präsenzübung 2a

Voraussetzungen: Bis einschließlich Abschnitt 4.

Übung 5. Beweise: Es gibt nur einen Primzahldrilling, d.h. nur eine Zahl p, so daß $p+2$ und $p+4$ auch Primzahlen sind.

Tip: Betrachten Sie Teilbarkeit durch 3 und mache eine Fallunterscheidung.

Übung 6. Zeige $2^n \geq n$ für alle $n \in N$ mit $n \geq 1$.

Präsenzübung 2b

Voraussetzungen: Bis einschließlich Abschnitt 4.

Übung 7. Finden Sie eine Formel für die Summe der Quadratzahlen $1^2 + \ldots + n^2$ und beweisen Sie sie per Induktion!

Tip: Die Formel sollte ein Polynom in n sein, welches ausmultipliziert keine höheren Potenzen als n^3 enthält.

Übung 8. Was ist der Fehler in dem „Induktionsbeweis" von „alle Pferde haben die gleiche Farbe"?

Präsenzübung 3a

Voraussetzungen: Bis einschließlich Abschnitt 5.a.

Übung 9. Wir bilden eine beliebige Zahl aus 300 Mal der Ziffer 4 und 100 Mal der Ziffer 0. Zeigen Sie, daß diese Zahl keine Quadratzahl ist!

Tip: Welche Teilbarkeitsregel korrespondiert zur Quersumme?

Übung 10.

(i) Warum ist die Folge $[a]^1, [a]^2, [a]^3, [a]^4, \ldots$ für jedes a beim Teilen durch eine Zahl k periodisch?

(ii) Ermitteln Sie die Periode für $a = 2$ und $k = 9$.