Einleitung [1]

Wie der Name schon sagt sind Äquivalenzrelationen besondere Relationen. Deswegen erkläre ich hier ganz allgemein, was Relationen sind, anschließend hebe ich drei besondere Eigenschaften von Relationen hervor. Mit diesen drei Eigenschaften werden die Äquivalenzrelationen definiert. Mittels Äquivalenzrelationen werden dann Äquivalenzklassen definiert.

Im Anschluss gebe ich einige wichtige Eigenschaften von Äquivalenzklassen und ein paar Beispiele an.

1 Definition von Relation, Äquivalenzrelation und Äquivalenzklassen

Definition 1.1 *Eine* **Relation** R *auf der Menge* M *ist eine Teilmenge* $R \subset M \times M$*. Man sagt zwei Elemente* m_1 *und* m_2 *von* M *stehen in Relation* R *zueinander, falls* $(m_1,m_2) \in R$*.*

Definition 1.2 *Eine Relation* R *auf der Menge* M *heißt* **reflexiv**, *falls* $\forall\, m \in M$ *gilt:* $(m, m) \in R$*.*

Definition 1.3 *Eine Relation* R *auf der Menge* M *heißt* **symmetrisch**, *falls gilt:* $(m_1, m_2) \in R \Rightarrow (m_2, m_1) \in R$*.*

Definition 1.4 *Eine Relation* R *auf der Menge* M *heißt* **transitiv**, *falls gilt:* $(m_1, m_2) \in R$ *und* $(m_2, m_3) \in R \Rightarrow (m_1, m_3) \in R$*.*

Definition 1.5 *Eine Relation heißt* **Äquivalenzrelation**, *falls sie reflexiv, symmetrisch und transitiv ist.*

Schreibweise: anstelle von (x, y) oder xRy ist die Schreibweise $x \sim y \pmod{R}$ oder auch nur $x \sim y$ gebräuchlich. Man sage x und y sind äquivalent.

Wir betrachten nun die Gesamtheit aller Elemente $m' \in M$, die zu m äquivalent sind, das ist die Äquivalenzklasse von m:

Definition 1.6 *Es sei* $m \in M$ *und* $\sim$ *sei eine Äquivalenzrelation auf* M*. Die Teilmenge*

$$[m] := \left\{\, m' \in M \;\middle|\; m' \sim m \,\right\} \subset M$$

heißt die **Äquivalenzklasse** *von* m *bzgl.* $\sim$*.*

Die Gesamtheit aller Äquivalenzklassen bekommt ebenfalls ein eigenes Symbol:

[1] Die ersten beiden Abschnitte sind eine Zusammenfassung der Abschnitte zu Äquivalenzrelationen bzw. Äquivalenzklassen in [Mey80] und [Beu00].

Definition 1.7 *Es sei $\sim$ bzw. R eine Äquivalenzrelation auf der Menge M, dann bezeichnet*

$$X/R = X/\sim \; := \{\, [m] \mid m \in M \,\}$$

die Menge aller Äquivalenzklassen von M.

2 Eigenschaften der Äquivalenzklassen

Beim Übergang von Elementen einer Menge zu den Äquivalenzklassen werden alle Elemente als gleichwertig angesehen, die zueinander äquivalent sind. Dabei werden alle Eigenschaften wegrationalisiert, die nichts mit der Äquivalenzrelation zu tun haben.

In diesem Abschnitt werden einige Eigenschaften angegeben, die die Nützlichkeit der obigen Begriffe unterstreichen.

Satz 1.8 Zwei äquivalente Element haben dieselbe Äquivalenzklasse:

$$m_1 \sim m_2 \Rightarrow [m_1] = [m_2]$$

Beweis: Wir zeigen $[m_1] \subset [m_2]$: es sei $m_3 \in [m_1]$ dann ist $m_3 \sim m_1$ und wegen der Transitivität gilt auch $m_3 \sim m_2$. Das heißt aber nichts anderes als $m_3 \in [m_2]$.

Um die Inklusion $[m_2] \subset [m_1]$ zu zeigen gehen wir analog vor. □

Satz 1.9 Zwei Äquivalenzklassen sind entweder gleich oder disjunkt.

Beweis: Das zeigen wir mit dem vorigen Satz. Wir betrachten zwei Äquivalenzklassen $[m_1]$ und $[m_2]$, sind sie nicht disjunkt, so gibt es ein $m_3 \in [m_1] \cap [m_2]$. Mit dem vorigen Satz folgt sofort $[m_1] = [m_3] = [m_2]$. Die beiden nicht-disjunkten Äquivalenzklassen sind gleich. □

Korollar 1.10 M ist die disjunkte Vereinigung seiner Äquivalenzklassen:

$$M = \bigcup_{m \in M} [m]$$

Beweis: Das folgt, da keine Äquivalenzklasse leer ist (wegen der Reflexivität ist ja $m \in [m]$) und jedes Element $m \in M$ in einer Äquivalenzklasse liegt. Die Disjunktheit folgt aus dem vorigen Satz. □

3 Beispiele für Äquivalenzklassen

3.1 Weltbevölkerung modulo Geschlecht

Wenn wir die Menschen in Männer und Frauen[2] unterteilen, erhalten wir eine Äquivalenzrelation und die Äquivalenzklassen sind [Man] und [Frau]. Und die Weltbevölkerung ist die disjunkte Vereinigung.

3.2 Schule modulo Schulklassen

Die Schüler einer Schule sind die disjunkte Vereinigung ihrer Schulklassen. Die Äquivalenzklassen sind die Schulklassen und zwei Schüler sind äquivalent, falls sie in der gleichen Klasse sind.

3.3 Die Restklassen mod m

Es sei $m \in \mathbb{N}, m > 0$. Zwei Zahlen $x, y \in \mathbb{Z}$ sind äquivalent falls gilt $x \equiv y \pmod{m}$. Schreibweise: $x \sim y$.

Die Äquivalenzklassen sind $m\mathbb{Z} + 0, m\mathbb{Z} + 1, m\mathbb{Z} + 2, \ldots, m\mathbb{Z} + (m-1)$, eine Äquivalenzklasse $m\mathbb{Z} + k, 1 \leq k \leq (m-1)$ ist die Menge $m\mathbb{Z} + k = \{ mz + k \mid z \in \mathbb{Z} \} = \{ \pm k, k \pm m, k \pm 2m, \ldots \}$. Die Menge aller Äquivalenzklassen ist

$$\mathbb{Z}/(m\mathbb{Z}) : \{ \mathbb{Z}m + k \mid k = 0, \ldots m-1 \}.$$

Eine andere Schreibweise ist: $\mathbb{Z}/\sim$, falls klar ist, dass $\sim$ Kongruenz modulo m bedeutet.

3.4 Gerade und ungerade Zahlen

Das ist ein Spezialfall des vorigen Beispiels: Kongruenz modulo 2. Aber man sieht hier sehr schön, dass die ganzen Zahlen die disjunkte Vereinigung der geraden und ungeraden Zahlen sind.

[2] Wir vernachlässigen die Existenz von Hermaphroditen.

4 Das Rechnen mit Kongruenzklassen

Es sei $m \in \mathbb{N}$, wir betrachten die Summe und das Produkt modulo m von zwei Zahlen $m_1, m_2 \in \mathbb{Z}$. Dazu schreiben wir die beiden Zahlen in der folgenden Art und Weise:

$$\begin{aligned} m_1 &= q_1 m + r_1 \\ m_2 &= q_2 m + r_2 \\ &\quad \text{mit } 0 \leq r_1, r_2 < m \text{ und } q_1, q_2 \in \mathbb{Z}\,. \end{aligned}$$

Für die Summe $m_1 + m_2$ stellen wir fest:

$$\begin{aligned} m_1 + m_2 &= q_1 m + r_1 + q_2 m + r_2 = (q_1 + q_2)m + r_1 + r_2 \\ &\equiv (r_1 + r_2) \pmod{m}. \end{aligned}$$

Für das Produkt $m_1 m_2$ gilt:

$$\begin{aligned} m_1 m_2 &= (q_1 m + r_1)(q_2 m + r_2) = q_1 q_2 m^2 + q_1 m r_2 + r_1 q_2 m + r_1 r_2 \\ &\equiv r_1 r_2 \pmod{m} \end{aligned}$$

Wenn wir mit Restklassen rechnen macht es daher keinen Unterschied, ob zuerst reduziert wird ($m_i \to r_i$) und dann gerechnet wird, oder ob die Reduktion nach der Rechnung erfolgt. Allerdings kann die Rechnung im ersten Fall erheblich reduziert werden.

Beispiel: Berechene $1001^{100} \pmod{1000}$. Zuerst reduziert: $1001 \equiv 1 \pmod{1000}$, dann potenziert (multipliziert): $(1 \pmod{1000})^{100} = 1 \pmod{1000}$.

Etwas extremer mit Pari/GP:

```
? #
   timer = 1 (on)
? Mod(1001^1000000,1000);
time = 509 ms.
? Mod(1001,1000)^1000000;
time = 0 ms.
```

Ein Beispiel zum Rechnen mit Restklassen: Ich greife hier noch einmal das Beispiel Aufgabe 2 vom dritten Übungsblatt auf. Es ist x so zu wählen, dass $7x+138 \equiv 0 \pmod{11}$ ist.

Es gibt mehrere Wege um x zu bestimmen:

Probieren: Man wählt x durch Probieren, so dass $7x + 138$ ein Vielfaches von 11 ist.

Diese Methode lässt sich etwas verfeinern indem man obigen Ratschlag beherzigt und zuerst modulo 11 reduziert. Das führt auf $7x+6$ soll ein Vielfaches von 11 sein ($138 = 110 + 22 + 6 \equiv 6 \pmod{11}$). Wir gehen systematisch die Vielfachen von 11 durch, subtrahieren 6 und schauen, ob ein Vielfaches von 7 dabei ist:

11*k	11*k-6	Vielfaches von 7?
11	5	nein
22	16	nein
33	27	nein
44	38	nein
55	49	ja: $7 \cdot 7$

x ist 7.

Alternativ hätten wir auch die Vielfachen von 7 probieren können, 6 addieren und schauen ob das ein Vielfaches von 11 ist.

x direkt bestimmen: $7x + 138 \equiv 0 \pmod{11} \Rightarrow 7x \equiv -138 \equiv -6 \pmod{11} \Rightarrow$ $x = -7^{-1}6 \pmod{11}$. Hier ließe sich x direkt ablesen, falls man das Inverse von 7 modulo 11 bestimmt hätte:

Probieren: 11 ist klein, man probiert für $y = 1, \ldots, 10$ solange bis $7y \equiv 1 \pmod{11}$ ist, also ein (1+Vielfaches von 11) ist: Man findet $7 * 3 = 21 \equiv -1 \pmod{11}$ daraus folgert man messerscharf: $7*3*-1$ ist dann $\equiv (-1)(-1) \equiv 1 \pmod{11}$ und -3 ist das multiplikative Inverse von 7. Es ist aber $-3 \equiv 8 \pmod{11}$. 8 ist ebenfalls multiplikatives Inverses. (-3 und 8 sind Repräsentanten der gleichen Äquivalenzklasse modulo 11).

Systematisch: Inverse kann man systematisch mit dem Satz von Bezout ausrechnen, auch für große Moduln. (Der Satz von Bezout ist der euklidische Algorithmus, der geht für kleine Zahlen auch ohne Computer):

```
? bezout(7,11)
%1 = [-3, 2, 1]
```

D.h. $7(-3) + 11 \cdot 2 = 1$.

Auf die eine oder andere Weise haben wir unser $7^{-1} \equiv 8 \pmod{11}$ bestimmt, x ist nun $x \equiv (-138)7^{-1} \equiv -6 \cdot 8 \equiv -48 \equiv 7 \pmod{11}$.

Literaturverzeichnis

[Beu00] Beutelspacher, A.: *Lineare Algebra – Eine Einführung in die Wissenschaft der Vektoren, Abbildungen und Matrizen.* 4., durchgesehene Auflage. Braunschweig : Vieweg, 2000. – ISBN 3–528–36508–0

[Mey80] Meyberg, K.: *Algebra, Teil 1.* 2. Auflage. München : Hanser, 1980 (Mathematische Grundlagen für Mathematiker, Physiker und Ingenieure)