$1 + 1 = 0$

Prof. Dr. Otmar Venjakob

Mathematisches Institut
Universität Bonn

Regionale Siegerehrung der 45. Mathematik-Olympiade, 2005

Zählen im Alltagsleben

Beim Zählen von Tieren, Gegenständen stoßen wir auf die **natürlichen Zahlen**

$$\mathbb{N}_{\geq 1} = \{1, 2, 3, \dots\},$$

die durch sukzessive Addition mit 1 entstehen:

$$\begin{aligned} 1 &, \\ 2 &= 1 + 1, \\ 3 &= 2 + 1, \dots \end{aligned}$$

Geschichtlich ist die *Erfindung* der 0 eine enorme kulturelle Leistung

$$\mathbb{N} = \{0, 1, 2, 3, \dots\},$$

Die ganzen Zahlen

Zur Umkehrung der Addition natürlicher Zahlen benötigt man zusätzlich die negativen Zahlen und gelangt so zu den **ganzen Zahlen**

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

$(\mathbb{Z}, +)$ nennen Mathematiker eine *Gruppe*:

$$\begin{aligned} a + 0 &= a \\ a + (-a) &= 0 \\ (a + b) + c &= a + (b + c) \end{aligned}$$

Die Welt der Mathematik

Auch wenn oft durch die *reale Welt* inspiriert,

ist das Gebäude der Mathematik rein *axiomatisch,*

d.h. eine ganz eigene Welt für sich, die ihren *eigenen Regeln* genügt - unabhängig von der Alltagswelt.

Zum Beispiel können wir uns selbst *neue* Gruppen definieren.

Division mit Rest

Für eine feste natürliche Zahl n betrachten wir

$$Z_n := \{0, 1, \ldots, n-1\}, \quad \text{etwa } Z_5 := \{0, 1, 2, 3, 4\}$$

Division mit Rest: Zu jeder ganzen Zahl m existiert genau ein $c(m)$ in Z_n und eine ganze Zahl $b(m)$ mit

$$m = b(m) \cdot n + c(m)$$

Beispiel: (für $n = 5$)

$$24 = 4 \cdot 5 + 4, \quad -3 = -1 \cdot 5 + 2, \quad 5 = 1 \cdot 5 + 0.$$

So ordnen wir jeder ganzen Zahl m eine Klasse $c(m)$ in Z_n zu.

Die neue Gruppe

Wir erklären eine (neue) Addition auf der Menge Z_n :

$$a + b = c(a + b)$$

für a, b in Z_n, d.h. wir addieren erst auf herkömmliche Weise und danach gehen wir zu der Klasse des Zwischenergebnisses über.

Beispiel: $(n = 5)$

$$2 + 2 = c_5(4) = 4,$$
$$4 + 3 = c_5(7) = 2,$$
$$3 + 2 = c_5(5) = 0,$$

d.h.

$$-3 = 2$$

in der Gruppe $(Z_5, +)$.

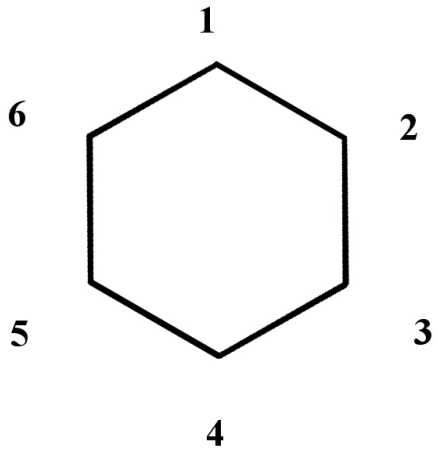
Für $n = 2$ ergibt sich also

$$1 + 1 = c_2(2) = 0$$

in der Gruppe $Z_2 = \{0, 1\}$.

Das regelmäßige n-Eck

Betrachten wir das regelmäßige n-Eck, etwa für $n = 6$:



Drehungen d_1 um $60 = \frac{360}{6}$ Grad bilden E_6 auf sich selbst ab (Ecke 1 $\mapsto$ Ecke 2, Ecke 2 $\mapsto$ Ecke 3, usw. , Ecke 6 $\mapsto$ Ecke 1).

Drehungen

Allgemeiner betrachten wir die Menge D_6 aller Drehungen d, die E_6 auf sich abbilden. Zum Beispiel ist die (mehrfache) Hintereinanderausführung $\circ$ von Drehungen d_1 um 60 Grad wieder in D_6:

$$
\begin{aligned}
d_2 &:= d_1 \circ d_1 && \text{Drehung um 120 Grad} \\
d_3 &:= d_1 \circ d_1 \circ d_1 && \text{Drehung um 180 Grad} \\
&\vdots \\
d_k &:= \underbrace{d_1 \circ \cdots \circ d_1}_{k-\text{mal}} && \text{Drehung um } k \cdot 60 \text{ Grad}
\end{aligned}
$$

Tatsächlich sind alle Drehungen in D_6 von dieser Form:

$$D_6 = \{d_0, d_1, d_2, d_3, d_4, d_5\}$$

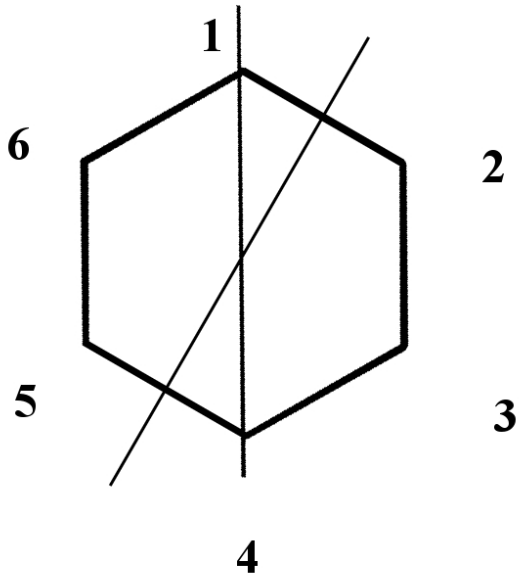
und $(D_6, \circ)$ hat dieselbe Gruppenstruktur wie $(Z_6, +)$:

$$d_a \leftrightarrow a,$$

$$d_a \circ d_b = d_{c_6(a+b)}.$$

Symmetriegruppen

Andere Symmetrien sind etwa durch *Spiegelungen* gegeben:



Die Gruppe aller Abbildungen der Ebene, die E_n in E_n überführt, heißt *Symmetriegruppe* von E_n.

Ähnlich kann man Symmetrien von **Yantras** studieren:

Mandalas

Anwendungen in Archäologie

In der **Archäologie** kann der Grad der Symmetrien (Größe der Symmetriegruppe) von Kachelmustern, Ornamenten etc. helfen, Fundstücke der richtigen Epoche zuzuordnen.

Elliptische Kurven

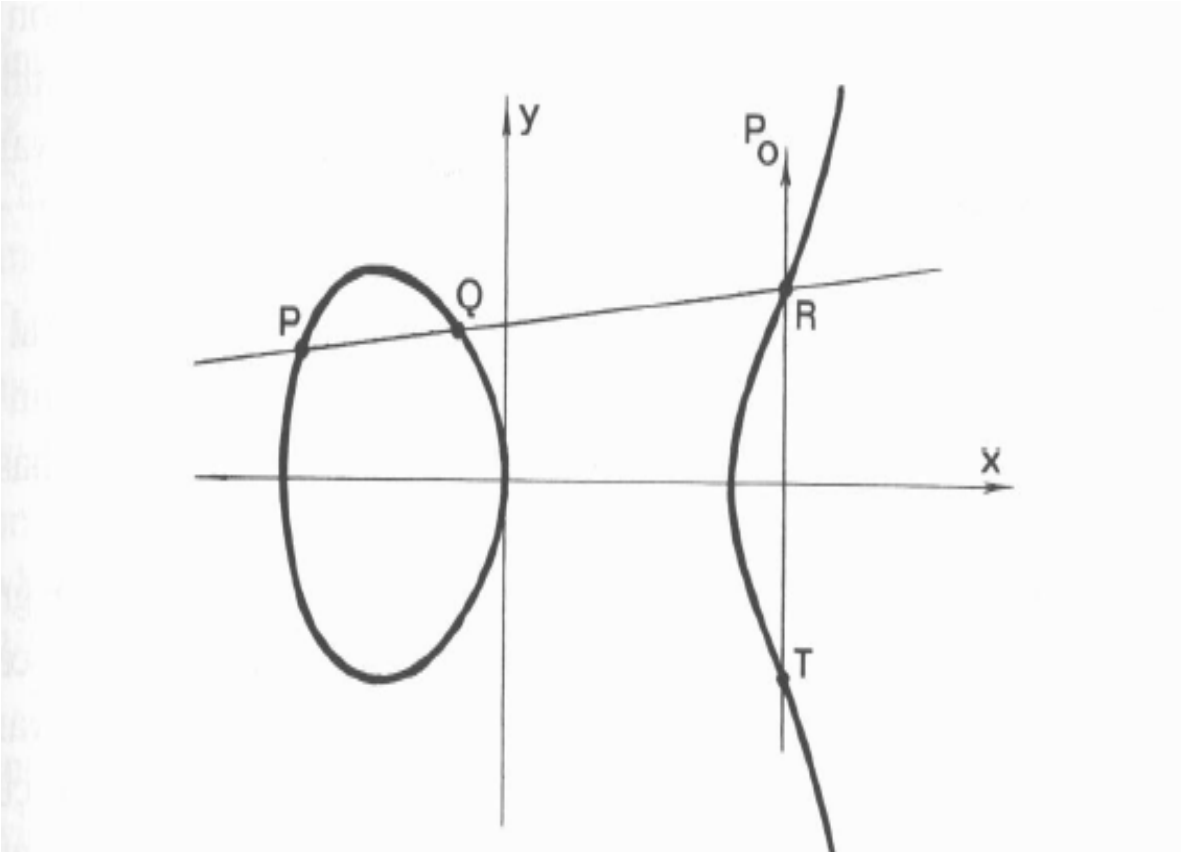
Schließlich noch eine außergewöhnliche, *geometrische* Addition: Wir betrachten die Gleichung

$$E : y^2 = x^3 - x.$$

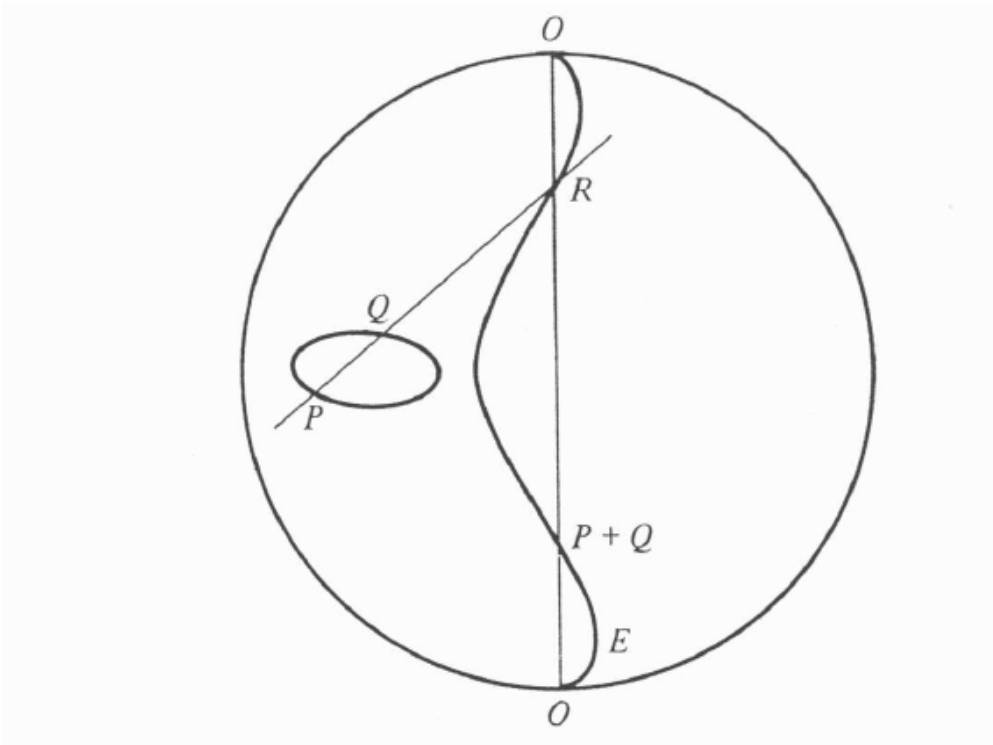
Die Lösungsmenge, d.h. Koordinaten (x, y), die E erfüllen, bilden ein geometrisches Objekt, eine *elliptische Kurve* E : $P_0 = (\infty, \infty) \in E$ spielt besondere Rolle:

$$P_0 = 0$$

$$E : y^2 = x^3 - x.$$



Geometrische Addition



Kryptographie

Elliptische Kurven spielen wichtige Rolle für

Verschlüsselungsverfahren

(Internet, EC-Karte, ...)