



Hochschule **RheinMain**
University of Applied Sciences
Wiesbaden Rüsselsheim

Kapitel 6

Algebraische Grundstrukturen

6.1 Gruppen

Definition, Beispiele: $(\mathbf{Z}, +)$, $(\mathbf{R} \setminus \{0\}, \cdot)$, $(\mathbf{Z}_n, +)$, (\mathbf{Z}_n^*, \cdot)

6.2 Ringe

Definition, Beispiele: $(\mathbf{Z}, +, \cdot)$, $(\mathbf{Z}_n, +, \cdot)$, Polynome

6.3 Körper

Definition, Beispiele: \mathbf{Q} , \mathbf{R} , \mathbf{Z}_p und $\text{GF}(p^n)$

6.1 Gruppen



Gruppen

Definition. Eine **Gruppe** (G, \circ) besteht aus einer Menge G zusammen mit einer Verknüpfung \circ , so dass folgende Gesetze erfüllt sind:

(G0) Abgeschlossenheit: Die Verknüpfung \circ ordnet je zwei Elementen $g, h \in G$ wieder ein Element $g \circ h \in G$ zu.

(G1) Assoziativität: Die Verknüpfung \circ ist assoziativ: Für alle $g, h, k \in G$ gilt $(g \circ h) \circ k = g \circ (h \circ k)$.

(G2) Existenz eines neutralen Elements: Es gibt ein Element aus G , das wir e nennen, für das gilt: $e \circ g = g \circ e = g$ für alle $g \in G$.

(G3) Existenz inverser Elemente: Für jedes $g \in G$ gibt es ein Element aus G , das wir g^{-1} nennen, für das gilt: $g^{-1} \circ g = g \circ g^{-1} = e$.

Wenn zusätzlich das folgende Axiom (G4) gilt, nennt man eine Gruppe G (**kommutativ** oder) **abelsch**:

(G4) Kommutativität: Für je zwei Elemente $g, h \in G$ gilt $g \circ h = h \circ g$.

Bemerkungen:

- Manchmal nennt man das neutrale Element auch 1.
- Manchmal ist es natürlich, die Verknüpfung einer Gruppe *additiv* zu schreiben. Dann bezeichnen wir das neutrale Element mit 0 und das zu g inverse Element mit $-g$.

Die Gruppe $(\mathbb{Z}, +)$

Die Menge der ganzen Zahlen \mathbb{Z} bildet mit der Verknüpfung „ $+$ “ (Addition) eine abelsche Gruppe, denn:

(G0) *Abgeschlossenheit*: Die Summe zweier ganzen Zahlen ist wieder eine ganze Zahl: Für alle $x, y \in \mathbb{Z}$ ist $x + y \in \mathbb{Z}$.

(G1) *Assoziativität*: Die Addition ist assoziativ: Für alle $x, y, z \in \mathbb{Z}$ gilt $(x + y) + z = x + (y + z)$.

(G2) *Existenz eines neutralen Elements*: Es gibt ein Element in \mathbb{Z} , nämlich 0, für das gilt: $0 + x = x + 0 = x$ für alle $x \in \mathbb{Z}$.

(G3) *Existenz inverser Elemente*: Für jedes $x \in \mathbb{Z}$ gibt es ein Element aus \mathbb{Z} , nämlich $-x$, für das gilt: $-x + x = x + (-x) = 0$.

(G4) *Kommutativität*: Für alle $x, y \in \mathbb{Z}$ ist $x + y = y + x$.

Die Gruppe $(\mathbb{R} \setminus \{0\}, \cdot)$

Die Menge $\mathbb{R} \setminus \{0\}$ der reellen Zahlen ungleich 0 bildet mit der Verknüpfung „ \cdot “ (Multiplikation) eine abelsche Gruppe, denn:

(G0) *Abgeschlossenheit*: Das Produkt zweier reeller Zahlen $\neq 0$ ist wieder eine reelle Zahl $\neq 0$.

(G1) *Assoziativität*: Die Multiplikation ist assoziativ.

(G2) *Neutrales Element* ist 1, denn $1 \cdot x = x \cdot 1 = x$ für alle $x \in \mathbb{R} \setminus \{0\}$.

(G3) *Inverses Element*: Für jede reelle Zahl $x \neq 0$ ist x^{-1} ($= 1/x$) das inverse Element, denn $x^{-1} \cdot x = x \cdot x^{-1} = 1$.

(G4) *Kommutativität*: Für alle $x, y \in \mathbb{R} \setminus \{0\}$ ist $x \cdot y = y \cdot x$.

KEINE Gruppen sind ...

KEINE Gruppen sind zum Beispiel:

(a) (\mathbb{R}, \cdot) ,

denn: 0 besitzt kein (multiplikativ) inverses Element, weil es für $x = 0$ keine reelle Zahl x^{-1} gibt, so dass $x^{-1} \cdot x = 1$.

(b) $(\mathbb{Z} \setminus \{0\}, \cdot)$,

denn: Zum Beispiel hat 2 kein (multiplikativ) inverses Element, weil es für $x = 2$ keine ganze Zahl x^{-1} , so dass $x^{-1} \cdot x = 1$ ist.

(c) $(\mathbb{N}, +)$,

denn: Alle natürlichen Zahlen $n > 0$ haben keine (additiv) inversen Elemente, weil es keine natürlichen Zahlen $-n$ gibt mit $-n + n = 0$.

Wir untersuchen nun *endliche* Strukturen.

Definition. Wir definieren die Menge Z_n als Menge aller natürlichen Zahlen, die kleiner als n sind:

$$Z_n = \{0, 1, \dots, n-1\}.$$

Um innerhalb dieser Menge addieren zu können, rechnen wir **modulo n**.

Beispiel: Um in $Z_6 = \{0, 1, 2, 3, 4, 5\}$ die Elemente 4 und 5 zu addieren, rechnen wir

$$4 + 5 \bmod 6 = 9 \bmod 6 = 3 \quad (= \text{Rest bei Division von 9 durch 6}).$$

Beispiel: Additionstafel von \mathbb{Z}_6

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Die Gruppe $(\mathbb{Z}_n, +)$

Satz. Mit der Addition modulo n bildet $(\mathbb{Z}_n, +)$ eine abelsche Gruppe.

(G0) Abgeschlossenheit: Da wir modulo n rechnen, ist für alle $x, y \in \mathbb{Z}_n$ die Summe wieder in $\{0, 1, \dots, n-1\}$, also $x + y \bmod n \in \mathbb{Z}_n$.

(G1) Assoziativität: Die Addition ist assoziativ: Für alle $x, y, z \in \mathbb{Z}_n$ gilt $(x + y \bmod n) + z \bmod n = x + (y + z \bmod n) \bmod n$.

(G2) Existenz eines neutralen Elements: Die Zahl $0 \in \mathbb{Z}_n$ ist das neutrale Element, denn: $0 + x \bmod n = x + 0 \bmod n = x$ für alle $x \in \mathbb{Z}_n$.

(G3) Existenz inverser Elemente: Für $x \in \mathbb{Z}_n$ ist $n-x \in \mathbb{Z}_n$ das inverse („negative“) Element, denn: $(n-x) + x \bmod n = n \bmod n = 0$.

(G4) Kommutativität: Für alle $x, y \in \mathbb{Z}_n$ ist $x + y \bmod n = y + x \bmod n$.

(\mathbb{Z}_n, \cdot) ist KEINE Gruppe

(\mathbb{Z}_n, \cdot) mit der Multiplikation modulo n ist KEINE Gruppe.

Denn: $0 \in \mathbb{Z}_n$ besitzt kein (multiplikativ) inverses Element, weil es keine Zahl $x \in \mathbb{Z}_n$ gibt mit $0 \cdot x = 1$.

Im Allgemeinen besitzen auch weitere Elemente aus \mathbb{Z}_n keine multiplikativen Inversen.

Beispiel: In \mathbb{Z}_6 haben die Elemente 0, 2, 3 und 4 keine (multiplikativen) Inversen. Dies kann man an der Multiplikationstafel von \mathbb{Z}_6 erkennen (siehe nächste Folie).

Beispiel: Multiplikationstafel von \mathbb{Z}_6

.	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Nur eine gewisse Teilmenge von Z_n bildet mit der Multiplikation modulo n eine Gruppe.

Definition. Die Menge Z_n^* besteht aus den Elementen von Z_n , die *teilerfremd* zu n sind, also

$$Z_n^* = \{x \in Z_n \mid x \text{ und } n \text{ sind teilerfremd}\}.$$

Beispiele:

- (a) $Z_6^* = \{1, 5\}$
- (b) $Z_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$
- (c) Wenn p eine Primzahl ist, gilt $Z_p^* = \{1, 2, 3, 4, \dots, p - 1\} = Z_p \setminus \{0\}$.

Übung

$$\mathbf{Z}_{21}^* =$$

Multiplikation in \mathbf{Z}_n^*

Auch in \mathbf{Z}_n^* wird **modulo n** multipliziert.

Beispiel: Die Multiplikationstafel von $\mathbf{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$ ist

.	1	2	4	7	8	11	13	14
1	1	2	4	7	8	11	13	14
2	2	4	8	14	1	7	11	13
4	4	8	1	13	2	14	7	11
7	7	14	13	4	11	2	1	8
8	8	1	2	11	4	13	14	7
11	11	7	14	2	13	1	8	4
13	13	11	7	1	14	8	4	2
14	14	13	11	8	7	4	2	1

Web-Tipp: Gruppentafeln online erstellen: <http://hobbes.la.asu.edu/groups/groups.html>

Abgeschlossenheit von \mathbb{Z}_n^*

Satz. \mathbb{Z}_n^* ist bezüglich der Multiplikation modulo n abgeschlossen.

Beweis: Seien x und y Elemente von \mathbb{Z}_n^* . Dann sind x und y teilerfremd zu n . Dann ist auch ihr Produkt $x \cdot y$ teilerfremd zu n (denn ein gemeinsamer Primteiler von $x \cdot y$ und n müsste auch x oder y teilen; also hätten auch x oder y und n einen gemeinsamen Primteiler). Also ist $x \cdot y \in \mathbb{Z}_n^*$. □

Für weitere Untersuchungen von \mathbb{Z}_n^* benötigen wir zwei Algorithmen aus der Zahlentheorie: den Euklidischen Algorithmus zur ggT-Berechnung und seine Erweiterung.

ggT

Seien a und b ganze Zahlen, die nicht beide 0 sind.

Unter allen Zahlen, die sowohl a als auch b teilen („gemeinsame Teiler von a und b “), gibt es eine größte. Diese nennen wir den **größten gemeinsamen Teiler**

ggT(a, b)

von a und b . Wenn a und b teilerfremd sind, ist $ggT(a, b) = 1$.

Beispiele:

- (a) 6 ist größter gemeinsamer Teiler von 12 und 18, denn die gemeinsamen Teiler sind 1, 2, 3, 6; unter diesen ist 6 am größten.
- (b) $ggT(20, 9) = 1$, denn 20 und 9 sind teilerfremd.

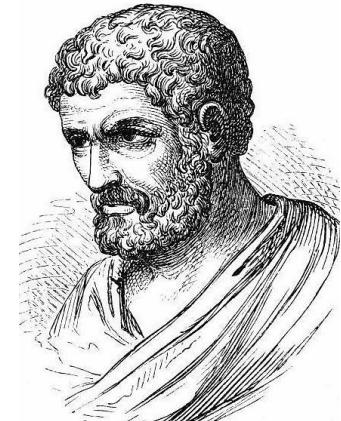
Euklidischer Algorithmus

Eine effiziente Berechnung des ggTs, auch von großen Zahlen, ermöglicht der

Euklidischer Algorithmus (Euklid, ca. 300 v. Chr.).

Seien a und b ganze Zahlen mit $b > 0$.

Dann kann man den $\text{ggT}(a, b)$ wie folgt bestimmen:



1. Schritt (Division mit Rest): Berechne die Zahlen q und r mit $a = q \cdot b + r$ und $0 \leq r < b$.

2. Schritt (Wiederholung mit neuem a und b): Wenn $r \neq 0$ ist, dann setze $a := b$ und $b := r$ und führe erneut den 1. Schritt durch.

Wenn $r = 0$ ist, dann ist b der gesuchte ggT.

Beispiel: Euklidischer Algorithmus

Wir können den ggT zweier natürlichen Zahlen wie folgt bestimmen:

- Wiederholte Division mit Rest.
- Der ggT ist der letzte von Null verschiedene Rest.

Beispiel: Euklidischer Algorithmus, um den ggT(91, 8) zu bestimmen:

$$91 = 11 \cdot 8 + 3$$

$$8 = 2 \cdot 3 + 2$$

$$3 = 1 \cdot 2 + 1$$

$$2 = 2 \cdot 1 + 0$$

Also ist **ggT(91, 8) = 1**, d.h. 91 und 8 sind teilerfremd.

Übung

Berechnen Sie den $\text{ggT}(31, 23)$ mit dem Euklidischen Algorithmus.

Lemma von Bézout

Lemma von Bézout. Seien a und b ganze Zahlen, und sei $d = \text{ggT}(a, b)$. Dann gibt es ganze Zahlen a' und b' mit

$$d = a \cdot a' + b \cdot b'.$$

Insbesondere gilt: Wenn a und b *teilerfremd* sind, gibt es ganze Zahlen a' und b' mit

$$1 = a \cdot a' + b \cdot b'.$$



Diese Darstellung nennt man auch **Vielfachsummendarstellung**.

Beispiel: Es gilt $\text{ggT}(8, 5) = 1$. Mit $a' = 2$, $b' = -3$ folgt

$$1 = 2 \cdot 8 + (-3) \cdot 5.$$

Erweiterter Euklidischer Algorithmus

Die Berechnung der Zahlen a' und b' der Vielfachsummandarstellung ist mit dem **erweiterten euklidischen Algorithmus** möglich.

Er beruht auf dem „Zurückrechnen“ des Euklidischen Algorithmus:

- 1. Schritt:** Mit dem euklidischen Algorithmus berechnen wir den $\text{ggT}(a, b)$.
- 2. Schritt:** Vom ggT ausgehend dröseln wir die Gleichungen „von unten nach oben“ der Reihe nach auf. (Achtung: Nicht zu viel ausmultiplizieren, nur die jeweiligen Reste ersetzen!)

Beispiel: Erweiterter Euklidischer Algorithmus

Euklidischer Algorithmus, um den $\text{ggT}(91, 8)$ zu bestimmen:

$$91 = 11 \cdot 8 + 3$$

$$8 = 2 \cdot 3 + 2$$

$$3 = 1 \cdot 2 + 1$$

$$2 = 2 \cdot 1 + 0 \quad \text{Also ist } \text{ggT}(91, 8) = 1.$$

Erweiterter euklidischer Algorithmus, um u und v mit $1 = 91u + 8v$ durch „Zurückrechnen“ zu finden:

$$1 = 3 - 1 \cdot 2$$

$$= 3 - 1 \cdot (8 - 2 \cdot 3) = 3 \cdot 3 - 1 \cdot 8$$

$$= 3 \cdot (91 - 11 \cdot 8) - 1 \cdot 8 = 3 \cdot 91 - 34 \cdot 8. \quad \text{Also: } u = 3, v = -34.$$

Übung

Bestimmen Sie die Vielfachsummendarstellung des $\text{ggT}(17, 5)$.

Inverse in \mathbf{Z}_n^*

Satz. Jedes Element von \mathbf{Z}_n^* hat eine (multiplikative) Inverse.

Beweis: Seien $x \in \mathbf{Z}_n^*$. Dann sind x und teilerfremd, also $\text{ggT}(x, n) = 1$.

Nach dem **Lemma von Bezout** gibt es ganze Zahlen x' und n' , so dass der ggT (hier: 1) durch folgende **Vielfachsumme** dargestellt werden kann:

$$1 = x' \cdot x + n' \cdot n.$$

mod n ergibt sich: $1 = x' \cdot x + n' \cdot n \pmod{n}$

$$1 = x' \cdot x + 0 \pmod{n}$$

$$1 = x' \cdot x \pmod{n}.$$

Also ist x' das (multiplikativ) inverse Element von x .

Berechnung der Inversen in \mathbf{Z}_n^*

Beispiel: Gesucht ist das inverse Element von $x = 35$ in \mathbf{Z}_{101}^* .

Erster Schritt: Berechnung des **ggT**(101, 35) mit dem **euklidischen Algorithmus**:

$$101 = 2 \cdot 35 + 31$$

$$35 = 1 \cdot 31 + 4$$

$$31 = 7 \cdot 4 + 3$$

$$4 = 1 \cdot 3 + 1$$

$$3 = 3 \cdot 1 + 0.$$

Also ist $\text{ggT}(101, 35) = 1$ (also liegt $x = 35$ tatsächlich in \mathbf{Z}_{101}^*).

Berechnung der Inversen in \mathbb{Z}_n^*

Zweiter Schritt: Um die **Vielfachsummendarstellung** zu erhalten, lösen wir die Gleichungen „von unten nach oben“ auf (**erweiterter euklidischer Algorithmus**):

$$\begin{aligned} 1 &= 4 - 1 \cdot 3 \\ &= 4 - 1 \cdot (31 - 7 \cdot 4) \\ &= 4 - 1 \cdot 31 + 7 \cdot 4 = 8 \cdot 4 - 1 \cdot 31 \\ &= 8 \cdot (35 - 1 \cdot 31) - 1 \cdot 31 = 8 \cdot 35 - 9 \cdot 31 \\ &= 8 \cdot 35 - 9 \cdot (101 - 2 \cdot 35) \\ &= \mathbf{26 \cdot 35 - 9 \cdot 101}. \end{aligned}$$

Modulo 101 ergibt sich $1 = 26 \cdot 35 - 9 \cdot 101 \pmod{101} = 26 \cdot 35 \pmod{101}$.
Also ist $x^{-1} = \mathbf{26}$ das Inverse von $x = 35$.

Übung

Berechnen Sie das inverse Element von $x = 13$ in \mathbf{Z}_{64}^* .

Die Gruppe (\mathbb{Z}_n^*, \cdot)

Die Multiplikation modulo n in \mathbb{Z}_n^* ist offensichtlich assoziativ und kommutativ (denn sie ist in \mathbb{Z}_n assoziativ und kommutativ).

Außerdem ist 1 das (multiplikativ) neutrale Element.

Insgesamt haben wir alle Gruppengesetze (G0) bis (G4) für \mathbb{Z}_n^* nachgewiesen.

Folgerung. Mit der Multiplikation modulo n ist (\mathbb{Z}_n^*, \cdot) eine abelsche Gruppe.

Weitere Gruppen

Auch viele andere Objekte können Gruppen bilden.

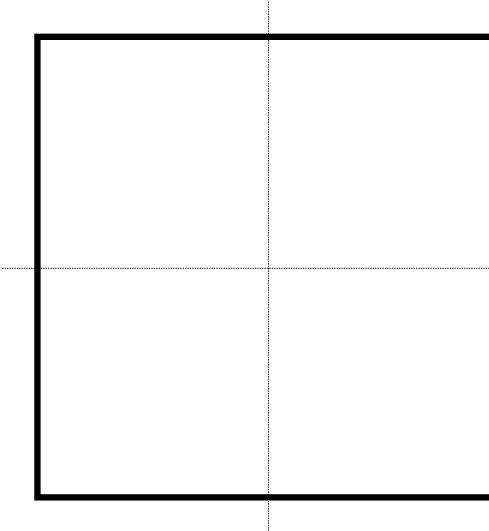
Beispiele:

- Permutationen (= bijektive Abbildungen endlicher Mengen in sich) bzgl. ihrer Hintereinanderausführung („**symmetrische Gruppe S_n** “)
- $m \times n$ -Matrizen bzgl. ihrer Addition
- $n \times n$ -Matrizen M mit $\det(M) \neq 0$ bzgl. ihrer Multiplikation („**General Linear Group**“)
- Geometrische Objekte mit ihren Symmetrieeabbildungen („**Symmetriegruppen**“)

Beispiel: Symmetriegruppe eines Quadrats

Die **Symmetriegruppe eines Quadrats** besteht aus allen Abbildungen, die ein Quadrat in sich überführen. Sie besteht aus

- der Identität,
- zwei Spiegelungen an den Diagonalen
- zwei Spiegelungen an den Geraden, die zwei gegenüberliegende Seitenmitten verbinden,
- Drehungen um 90° ,
- eine Drehung um 180° .



Beispiel: Zauberwürfel

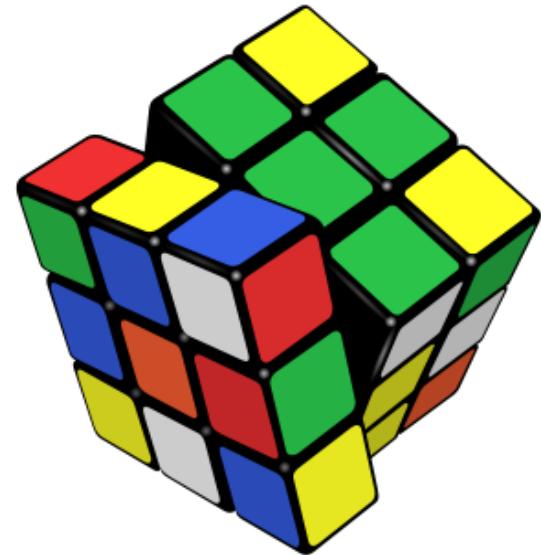
Die verschiedenen Verdrehungen des **Zauberwürfels (Rubik's Cube)** bilden ebenfalls eine endliche Gruppe.

Sie enthält

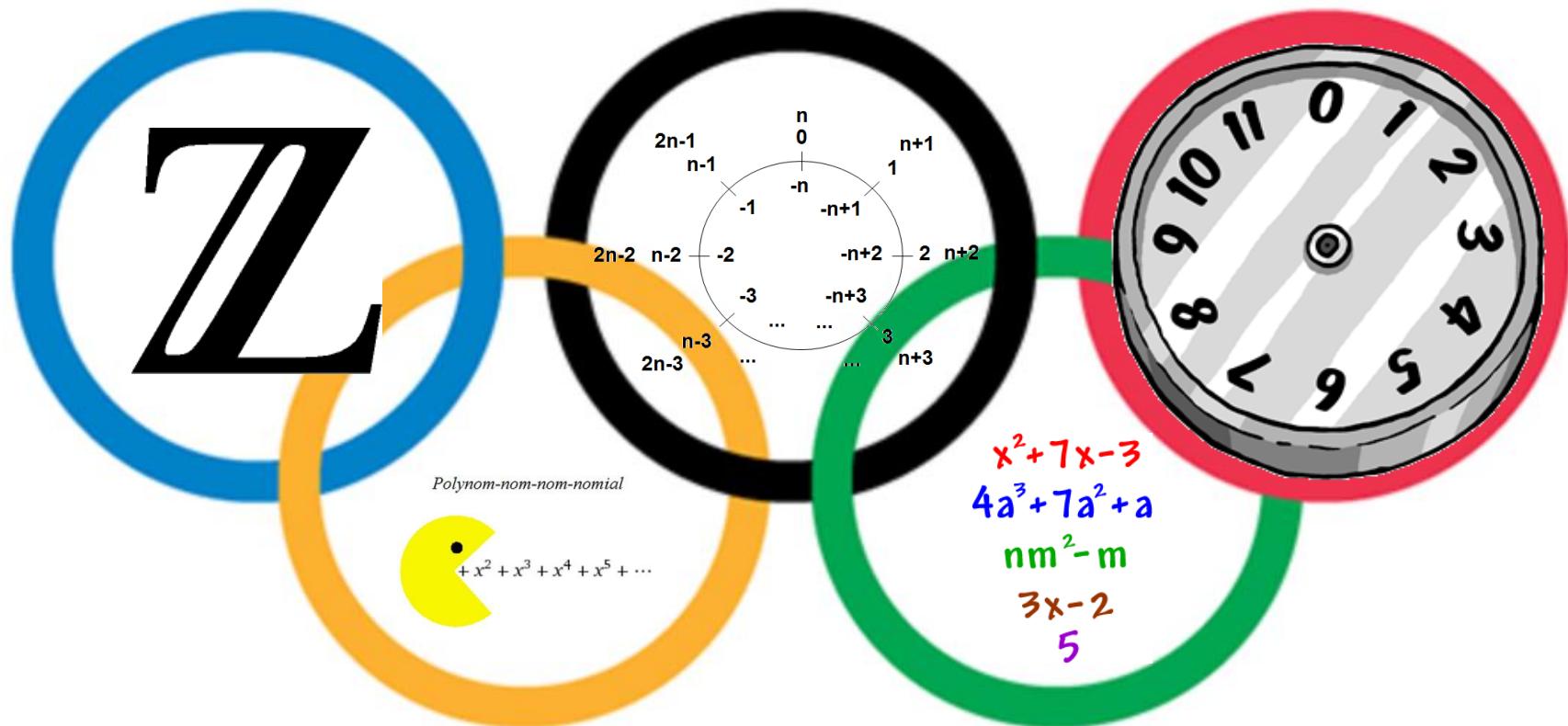
$$43.252.003.274.489.856.00 \approx 4,3 \cdot 10^{19}$$

Elemente.

Mit Hilfe der Gruppentheorie konnte 2014 gezeigt werden, dass man den Würfel immer mit höchstens 26 Drehungen lösen kann.



6.2 Ringe



Definition Ring

Idee: Ringe sind Strukturen, in denen man *addieren und multiplizieren* kann, in der jedoch ein Element nicht notwendigerweise ein multiplikatives Inverses hat.

Definition. Ein **Ring** ist eine Menge R zusammen mit zwei Verknüpfungen $+$ und \cdot , so dass die folgenden drei Gruppen von Gesetzen für alle Elemente $x, y, z \in R$ erfüllt sind:

1. Gesetze der Addition: $(R, +)$ ist eine abelsche Gruppe, d.h. es gilt:

Abgeschlossenheit: $x + y \in R$.

Assoziativität: $(x + y) + z = x + (y + z)$.

Definition Ring

Neutrales Element: Es gibt ein Element 0 von R („**Nullelement**“), für das gilt $0 + x = x$.

Inverser Elemente: Zu jedem x gibt es ein Element $-x$ („**negatives Element**“), für das gilt $x + (-x) = 0$.

Kommutativität: $x + y = y + x$.

2. Gesetze der Multiplikation:

Abgeschlossenheit: $x \cdot y \in R$.

Assoziativität: $x \cdot (y \cdot z) = (x \cdot y) \cdot z$

3. Distributivgesetze:

$$x \cdot (y + z) = x \cdot y + x \cdot z \text{ und } (x + y) \cdot z = x \cdot z + y \cdot z.$$

Der Ring \mathbb{Z}

Die Menge \mathbb{Z} der ganzen Zahlen ist zusammen mit der gewöhnlichen Addition und Multiplikation ein Ring.

Der Ring \mathbb{Z} erfüllt offensichtlich alle geforderten Gesetze für Ringe.

Darüber hinaus hat der Ring \mathbb{Z} ein neutrales Element der Multiplikation („Einselement“) (nämlich die Zahl 1) und auch die Multiplikation ist kommutativ.

Bemerkung: In \mathbb{Z} haben nur die Elemente 1 und -1 ein multiplikatives Inverses.

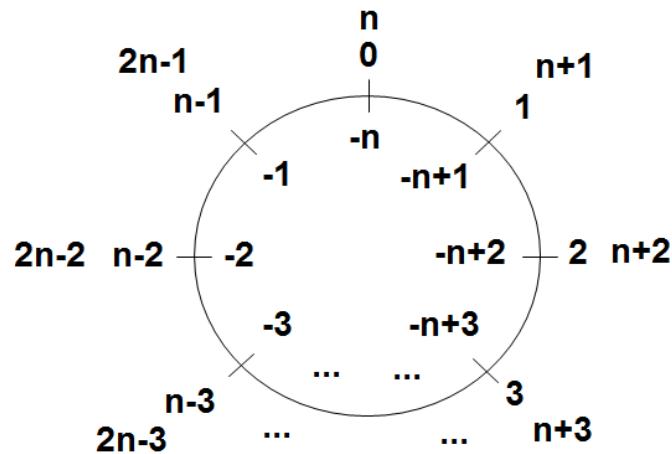
Der Ring \mathbf{Z}_n

Wir wissen bereits, dass die Struktur $\mathbf{Z}_n = \{0, 1, \dots, n-1\}$ mit der Addition modulo n eine additive Gruppe bildet.

Die Menge \mathbf{Z}_n ist zusammen mit der Addition und Multiplikation modulo n ein Ring. Dieser Ring hat ein Einselement und ist kommutativ.

Man nennt \mathbf{Z}_n auch den
Restklassenring modulo n .

Man kann sich \mathbf{Z}_n auch anschaulich
als „Ring“ vorstellen.



Beispiel: Der Ring \mathbb{Z}_{12}



Anwendung: Public-Key-Kryptografie mit RSA



Der Polynomring $R[x]$

Die Menge aller Polynome

$$f(x) = a_0 + a_1 \cdot x + a_2 \cdot x^2 + \dots + a_n \cdot x^n$$

mit reellen Koeffizienten a_i bildet mit der üblichen Addition und Multiplikation einen Ring.

Er heißt **Polynomring $R[x]$** in der Unbekannten x .

Dieser Ring hat außerdem ein Einselement und die Multiplikation ist kommutativ.

Die einzigen multiplikativ invertierbaren Polynome aus $R[x]$ sind die konstanten Polynome $f(x) = c \in R \setminus \{0\}$.

(Polynom-) Division

Sowohl die ganzen Zahlen \mathbb{Z} als auch die Polynome $\mathbb{R}[x]$ bilden einen (unendlichen) Ring (mit Einselement und kommutativer Multiplikation).

Auf dieser strukturellen Verwandtschaft beruht auch die Ähnlichkeit von ganzzahliger Division und Polynomdivision.

$$\begin{array}{r}
 62228 : 47 = 1324 \\
 \underline{-47} \downarrow \quad \leftarrow 47 \cdot 1 \\
 152 \\
 \underline{-141} \downarrow \quad \leftarrow 47 \cdot 3 \\
 112 \\
 \underline{-94} \quad \leftarrow 47 \cdot 2 \\
 188 \\
 \underline{-188} \quad \leftarrow 47 \cdot 4 \\
 0
 \end{array}$$

$$\begin{array}{rcl}
 \left(x^3 - 6x^2 + 11x - 12 \right) : (x-4) & = & x^2 - 2x + 3 \\
 \underline{- \left(x^3 - 4x^2 \right)} & \xrightarrow{\hspace{1cm}} & (x-4) \cdot x^2 \\
 -2x^2 + 11x & & \\
 \underline{- \left(-2x^2 + 8x \right)} & \xrightarrow{\hspace{1cm}} & (x-4) \cdot (-2x) \\
 3x - 12 & & \\
 \underline{- \left(3x - 12 \right)} & \xrightarrow{\hspace{1cm}} & (x-4) \cdot 3 \\
 0 & &
 \end{array}$$

ggT von Polynomen

Analog zu den ganzen Zahlen kann man bei Polynomen einen **größten gemeinsamen Teiler** (ggT) berechnen.

Beispiel: ggT($x^4 - 2x^3 + 2x^2 - 2x + 1$, $x^3 + x^2 - x - 1$) = ?

Euklidischer Algorithmus (fortgesetzte Polynomdivision mit Rest):

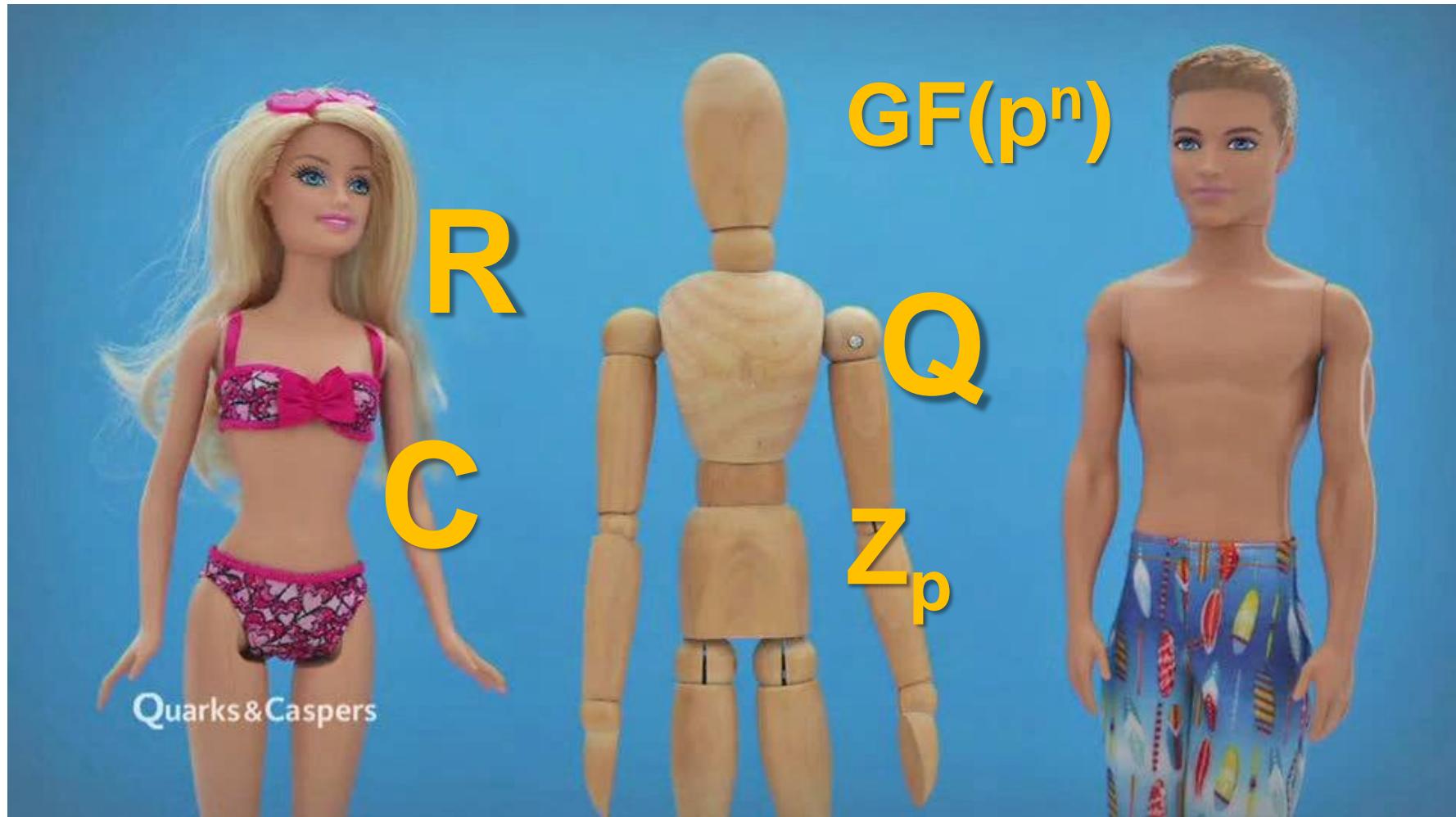
$$x^4 - 2x^3 + 2x^2 - 2x + 1 = (x - 3) \cdot (x^3 + x^2 - x - 1) + (6x^2 - 4x - 2)$$

$$x^3 + x^2 - x - 1 = (1/6x + 5/18) \cdot (6x^2 - 4x - 2) + (4/9x - 4/9)$$

$$6x^2 - 4x - 2 = (27/2x + 9/2) \cdot (4/9x - 4/9) + 0$$

Der gesuchte ggT ist gleich **$4/9x - 4/9$** (bzw. $x - 1$).

6.3 Körper



Körper

Grob gesagt sind (algebraische) Körper algebraische Strukturen, in denen man „wie gewohnt“ (wie in den reellen Zahlen) rechnen kann.

Definition. Eine Menge K mit $+$ und \cdot bildet einen **Körper**, wenn

- die beiden Operationen abgeschlossen sind,
- die beiden Operationen assoziativ und kommutativ sind,
- es ein neutrales Element 0 bzgl. der Addition und ein neutrales Element $1 \neq 0$ bezüglich der Multiplikation gibt,
- jedes Element x ein additives Inverses $-x$ und jedes Element $x \neq 0$ ein multiplikatives Inverses x^{-1} hat,
- das Distributivgesetz gilt.

Körper, Ringe, Gruppen

Wir können die Definition von Körpern auch mit Hilfe der Strukturen „Gruppe“ bzw. „Ring“ ausdrücken.

$(K, +, \cdot)$ ist ein **Körper**, wenn

- $(K, +)$ eine abelsche Gruppe (mit neutralem Element 0) ist,
- $(K \setminus \{0\}, \cdot)$ eine abelsche Gruppe ist und
- das Distributivgesetz gilt.

Bzw.

$(K, +, \cdot)$ ist ein **Körper**, wenn

- $(K, +, \cdot)$ ein Ring (mit neutralem Element 0) ist und
- $(K \setminus \{0\}, \cdot)$ eine abelsche Gruppe ist.

Beispiele für unendliche Körper

Folgende Beispiele für unendliche Körper sind uns vertraut:

- **Q = Körper der rationalen Zahlen** („Brüche“):
abbrechende oder periodische Dezimalzahlen
Beispiele: $\frac{1}{2} = 0,5$; $\frac{1}{3} = 0,\overline{3}$; $-\frac{5}{7} = -0,\overline{714285}$; ...
- **R = Körper der reellen Zahlen**:
alle Dezimalzahlen (auch unendliche, nichtperiodische)
Beispiele: π , e , $\sqrt{2}$, ...

Im nächsten Semester werden wir die obigen Zahlen noch erweitern:

- **C = Körper der komplexen Zahlen**

Endliche Körper

Es gibt auch Körper, die nur aus endlich vielen Elementen bestehen.

Einen solchen **endlichen Körper** mit n Elementen bezeichnet man auch als **GF(n)** (engl. „Galois Field“).

Endliche Körper spielen in der Kryptographie und in der Codierungs-theorie eine wichtige Rolle.

Vorteile beim Rechnen in endlichen Körpern sind zum Beispiel, dass es keine Rundungsfehler und keine Überläufe geben kann.

Frage: Für welche natürlichen Zahlen n existiert ein endlicher Körper mit n Elementen? Und wie sieht er aus?

Der kleinste Körper: \mathbb{Z}_2

Wir fangen klein an: Ein Körper muss mindestens die beiden Elemente 0 und 1 besitzen. Und dies genügt bereits!

Die Menge $\mathbb{Z}_2 = \{0, 1\}$ bildet einen Körper, wenn man die Addition und Multiplikation „**modulo 2**“ definiert.

+	0	1
0	0	1
1	1	0

.	0	1
0	0	0
1	0	1

Beachte: $1 + 1 \bmod 2 = 0$.

Der Körper \mathbb{Z}_3

Auch ein Körper mit 3 Elementen ist kein Problem.

Die Menge $\mathbb{Z}_3 = \{0, 1, 2\}$ bildet einen Körper, wenn man die Addition und Multiplikation „modulo 3“ definiert.

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

*	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Übung: Finden Sie (a) zu jedem Element das additiv Inverse:

$$-0 = \underline{\quad}, -1 = \underline{\quad}, -2 = \underline{\quad}$$

(b) zu jedem Element $\neq 0$ das multiplikativ Inverse: $1^{-1} = \underline{\quad}, 2^{-1} = \underline{\quad}$

Die Körper \mathbb{Z}_p

Körper, deren Elementanzahl eine Primzahl ist, sind sehr einfach zu konstruieren.

Satz. \mathbb{Z}_p ist mit der Addition und Multiplikation modulo p genau dann ein Körper, wenn p eine Primzahl ist.

Beweisidee. Wir wissen: \mathbb{Z}_p^* ist eine multiplikative Gruppe. Wenn p eine Primzahl ist, so ist $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$. Also besitzen alle Elemente aus \mathbb{Z}_p außer 0 ein multiplikatives Inverses. Also ist \mathbb{Z}_p ein Körper.

Ist n keine Primzahl, also z.B. $n = p \cdot q$, so ist \mathbb{Z}_n nicht „nullteilerfrei“: $p \cdot q \equiv 0 \pmod{n}$. Also ist \mathbb{Z}_n in diesem Fall kein Körper.

Beispiele: $\mathbb{Z}_{17} = \{0, 1, 2, \dots, 16\}$ ist mit $+$ und \cdot modulo 17 ein Körper. $\mathbb{Z}_{16} = \{0, 1, 2, \dots, 15\}$ ist mit $+$ und \cdot modulo 16 jedoch *kein* Körper.

Ein Körper mit 4 Elementen

\mathbb{Z}_4 mit $+$ und \cdot modulo 4 ist
kein Körper, denn z. B. hat 2
kein multiplikativ Inverses.

$+$	0	1	2	3	.	0	1	2	3
0	0	1	2	3	0	0	0	0	0
1	1	2	3	0	1	0	1	2	3
2	2	3	0	1	2	0	2	0	2
3	3	0	1	2	3	0	3	2	1

Trotzdem gibt es einen Körper mit 4 Elementen. **GF(4)** muss folgende Struktur haben:

$+$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

*	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

Existenz von endlichen Körpern

Welche endlichen Körper es gibt, klärt der folgende Satz.

Satz. Es gibt genau dann einen endlichen Körper mit q Elementen, wenn q eine Primzahlpotenz ist, d. h.

$$q = p^n,$$

wobei p eine Primzahl und n eine natürliche Zahl > 0 ist.

Für $q = p$, also $n = 1$, sind das die Körper \mathbb{Z}_p .

Für $q = p^n$ mit $n > 1$ sind diese Körper schwieriger zu konstruieren.

Übung

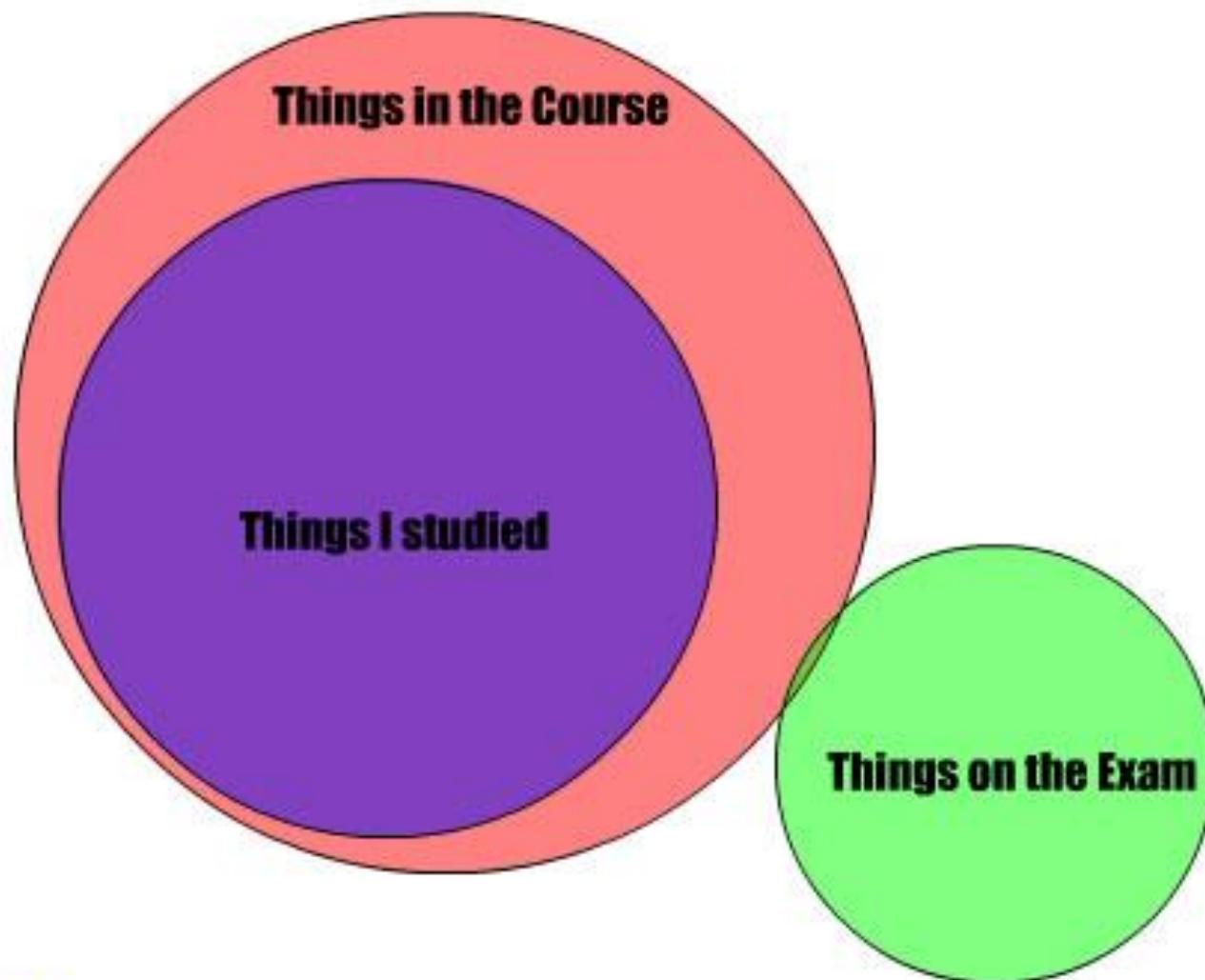
Kreuzen Sie an: Es gibt einen Körper mit ... Elementen.

- | | |
|-----------------------------|-----------------------------------|
| <input type="checkbox"/> 1 | <input type="checkbox"/> 11 |
| <input type="checkbox"/> 2 | <input type="checkbox"/> 12 |
| <input type="checkbox"/> 3 | <input type="checkbox"/> 13 |
| <input type="checkbox"/> 4 | <input type="checkbox"/> 14 |
| <input type="checkbox"/> 5 | <input type="checkbox"/> 15 |
| <input type="checkbox"/> 6 | <input type="checkbox"/> 16 |
| <input type="checkbox"/> 7 | <input type="checkbox"/> 1024 |
| <input type="checkbox"/> 8 | <input type="checkbox"/> 2016 |
| <input type="checkbox"/> 9 | <input type="checkbox"/> 1000000 |
| <input type="checkbox"/> 10 | <input type="checkbox"/> ∞ |

Danke für eure Aufmerksamkeit!

Noch Fragen?

Final Exams



**Don't
PANIC!**