Algebraische Strukturen Teil 1

Algebraische Strukturen

Algebraische Strukturen:

- Gruppen
- Ringe
- Körper
- Vektorräume (nächste Vorlesung)

Anwendungen:

- Public Key Verschlüsselungsverfahren
- Reed Solomon (nächste Vorlesung)

Algebraische Strukturen

Algebraische Strukturen:

Um was gehts hier?

Algebraische Strukturen

Eine algebraische Struktur ist schlicht eine **Menge**, auf der man eine oder mehrere **Operationen** ausführen kann.

Operation bedeutet **Verknüpfungen von Elementen**, also etwa Addition und Multiplikation.

Beispiel

Wenn wir zB 2+3 berechnen, dass ist das das Ausführen einer Operation auf zwei Gruppenelementen, zumindest wenn die Menge $\mathbb{Z}$ ist und die Addition so definiert ist, wie wir sie kennen.

Algebraische Strukturen

- Gruppen
- Ringe
- Körper
- Vektorräume

unterscheiden sich in den **Eigenschaften der Operationen** die auf der jeweiligen Struktur definiert sind.

Gruppen

Gruppen

Definition:
Eine **Gruppe** G besteht aus einer Menge G und einer Verknüpfung $*$ auf G mit den folgenden Eigenschaften:

(G1) Es gibt ein Element $e \in G$ mit der Eigenschaft
$e * a = a * e = a$ für alle $a \in G$.
e heißt **neutrales Element** in G.

(G2) Zu jedem $a \in G$ gibt es ein eindeutig bestimmtes Element
$a^{-1} \in G$ mit der Eigenschaft $a * a^{-1} = a^{-1} * a = e$.
a^{-1} heißt **inverses Element** zu a.

(G3) Für alle $a, b, c \in G$ gilt $a * (b * c) = (a * b) * c$.
G ist **assoziativ**.

Gruppen

Definition:
Die Gruppe $(G, *)$ heißt **kommutative Gruppe** oder **abelsche Gruppe**, wenn zusätzlich gilt:

(G4) Für alle $a, b \in G$ gilt $a * b = b * a$.

Gruppen

Beispiele:
$(\mathbb{R}, +)$ ist eine kommutative Gruppe mit neutralem Element $e = 0$ und inversem Element $a^{-1} = -a$.

Überprüfen wir die Eigenschaften:
(G1): $\forall a \in \mathbb{R}$ gilt natürlich $a + 0 = 0 + a = a$.
(G2): Ebenfalls wissen wir, dass $a + (-a) = (-a) + a = 0$ ist.
(G3): Auch $(a + b) + c = a + (b + c)$ akzeptieren wir sofort.

(G4): Wir behaupten, dass $(\mathbb{R}, +)$ kommutativ ist, dh $a + b = b + a$ gilt. Auch das sehen wir ein.

Hier ist der „Beweis“ quasi trivial, aber oft ist es etwas schwieriger.

Gruppen

Beispiele:
Ist $(\mathbb{R}^-, \cdot)$ eine Gruppe?

Überprüfen wir die Eigenschaften:
(G1) Gibt es in $\mathbb{R}^-$ ein neutrales Element bzgl. der Multiplikation? Wir wissen, dass das neutrale Element bzgl. Multiplikation 1 sein muss. Aber das neutrale Element muss selbst in G sein ($e \in G$), $1 \notin \mathbb{R}^-$, dh $(\mathbb{R}^-, \cdot)$ kann keine Gruppe sein.

$\Rightarrow$ Hier steckt die (nicht explizite erwähnte) Annahme drin, dass eine Gruppe **abgeschlossen** ist bzgl. ihrer Operation.

Gruppen

Satz:
Sei $(G, *)$ eine Gruppe, dann gilt für alle Elemente $a, b \in G$:

(a) Für das Inverse von $(a * b)$ gilt $(a * b)^{-1} = b^{-1} * a^{-1}$

(b) Das Inverse eines Elements a ist eindeutig.

Beweis:
(a) zu zeigen: $(a * b) * (b^{-1} * a^{-1}) = e$
$(a * b) * (b^{-1} * a^{-1}) = a * (b * b^{-1}) * a^{-1} = a * e * a^{-1} = a * a^{-1} = e$

Beachten Sie: $(a * b)^{-1} = a^{-1} * b^{-1}$ gilt nur in abelschen Gruppen.

Gruppen

Beweis von (b)

(b) zu zeigen: Sei a^{-1} und $\hat{a}$ Inverses zu a, dann gilt: $a^{-1} = \hat{a}$

$$a^{-1} = a^{-1} * e = a^{-1} * a * \hat{a} = (a^{-1} * a) * \hat{a} = e * \hat{a} = \hat{a}.$$

Gruppen

Satz/Definition:
Sei $U \subseteq G$ und $(G, *)$ eine Gruppe, dann ist $(U, *)$ eine Gruppe, wenn gilt:

$$a, b \in U \Rightarrow a * b \in U, a^{-1} \in U$$

U heißt dann **Untergruppe** von G.

Beweis:
$*$ ist eine Verknüpfung auf U, da ja $U \subseteq G$ und $*$ Verknüpfung auf G.

(G1) Es ist a und $a^{-1} \in U$, also auch $a * a^{-1} = e$. Dh $e \in G$

(G2) $a^{-1} \in U$ steckt schon in der Forderung.

(G3) $a * (b * c) = (a * b) * c$ stimmt für alle Elemente in G, also auch für $a, b, c \in U \subseteq G$, da für $a, b \in U$ gilt $a * b \in U$, folgt dass $a * (b * c) = (a * b) * c$ für alle $a, b, c \in U$ hält.

Gruppen

Beispiel

Wir haben gezeigt, dass $(\mathbb{R}, +)$ eine Gruppe ist. Wir behaupten nun, dass $(\mathbb{Z}, +)$ eine Untergruppe davon ist.

- $\mathbb{Z} \subseteq \mathbb{R}$ ist klar.
- $a + b \in \mathbb{Z}$ für alle $a, b \in \mathbb{Z}$ ist glaubwürdig.
- Für $a \in \mathbb{Z}$ gilt, dass das inverse Element $-a$ ist, und das ist ebenfalls in $\mathbb{Z}$.

Permutationsgruppen

Die bisherigen Beispiele sind eher trivial, da wir noch keinen interessanten Gruppen kennengelernt haben.

$\Rightarrow$ Permutationsgruppen

Weiß jeder was Permutationen sind?

Notation von Permutationen

Nehmen wir an wir haben eine Menge von Objekten $\{1, 2, 3, 4\}$ auf die wir eine Permutation ausführen. Die Elemente der Menge sind ursprünglich in einer bestimmten Reihenfolge angeordnet z. B $(1, 2, 3, 4)$. Als Ergebnis der Permutation sind sie anders gereiht, z. B. $\pi(1, 2, 3, 4) = (4, 3, 1, 2)$

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ \searrow & \swarrow & \searrow & \swarrow \end{pmatrix}$$

Alternativ schreiben wir auch oft $\pi = (1\ 3\ 2\ 4)$. Man kann dies lesen als „1 geht in 3 über, 3 in 2, 2 in 4 und 4 in 1“. 1 nimmt also den Platz von 3 ein.

Verkettung von Permutationen

Diese Schreibweise ist auch einfacher, wenn wir Permutationen nacheinander ausführen:

Wir haben $\pi_1 = (1\ 3\ 2)$ und $\pi_2 = (2\ 1\ 3)$ als Permutationen, die wir nacheinander ausführen wollen, also $(1\ 3\ 2) \circ (2\ 1\ 3)$.
Wichtig: Hier wird zuerst (2 1 3) ausgeführt und danach erst (1 3 2).

$(1\ 3\ 2) \circ (2\ 1\ 3)$ dh $1 \to 3 \& 3 \to 2$, also $1 \to 2$
$2 \to 1 \& 1 \to 3$, also $2 \to 3$
$3 \to 2 \& 2 \to 1$, also $3 \to 1$

$\Rightarrow (1\ 3\ 2) \circ (2\ 1\ 3) = (1\ 2\ 3)$

Permutationsgruppen

Wir haben gesehen, dass man Permutationen miteinander verknüpfen kann

Frage: Ist S_n eine Gruppe?
$S_n \ldots$ Die Menge der Permutationen, die sich auf n Elemente auswirken

(G1) Neutrales Element ist die Identität, also diejenige Permutation, die nichts verändert:
$\pi(a, b, \ldots, n) = (a, b, \ldots, n)$, also $\pi(i) = i$ für alle i

(G2) Inverses Element muss dasjenige sein, dass alles wieder auf seinen ursprünglichen Platz zurückbringt, also wenn gilt
$\pi(a) = b$, dann $\pi^{-1}(b) = a$

(G3) Assoziativität: $\pi_1 \circ (\pi_2 \circ \pi_3) = (\pi_1 \circ \pi_2) \circ \pi_3$
$\Rightarrow$ **Übungsaufgabe**

Permutationsgruppen

Permutationsgruppen sind also Gruppen. Wir betrachten nun S_3, also die Menge der Permutationen einer Menge mit drei Elementen.
Die **Verknüpfungstafel** lautet:

$\circ$	a	b	c	d	e	f
a	a	b	c	d	e	f
b	b	c	a	e	f	d
c	c	a	b	f	d	e
d	d	f	e	a	c	b
e	e	d	f	b	a	c
f	f	e	d	c	b	a

a ist klarerweise die Identität, und wenn man weiß, dass $b = (1\ 2\ 3)$ und $d = (2\ 3)$ ist, kann man die anderen Elemente berechnen.
Aufgabe: Berechnet die anderen Elemente!
Anmerkung: $d = (2\ 3)$ bedeutet, dass $1 \to 1$ abgebildet wird.

Permutationsgruppen

Auflösung:

$a = ()$
$b = (1\ 2\ 3)$
$c = (1\ 3\ 2)$
$d = (2\ 3)$
$e = (1\ 2)$
$f = (1\ 3)$

Anmerkungen:

- (1 3 2) ist dasselbe wie (3 2 1),
- die Tabelle ist so zu lesen: Zeile $i \odot$ Spalte j

Permutationsgruppen

$c = (1\ 3\ 2)$, denn $b \odot b = c$
$(1\ 2\ 3) \circ (1\ 2\ 3)$ dh $1 \to 2 \& 2 \to 3$, also $1 \to 3$
$2 \to 3 \& 3 \to 1$, also $2 \to 1$
$3 \to 1 \& 1 \to 3$, also $3 \to 3$

$d = (1\ 2)$, denn $b \odot d = e$
$(1\ 2\ 3) \circ (2\ 3)$ dh $1 \to 1 \& 1 \to 2$, also $1 \to 2$
$2 \to 3 \& 3 \to 1$, also $2 \to 1$
$3 \to 2 \& 2 \to 3$, also $3 \to 3$

$f = (3\ 1)$, denn $b \odot e = f$
$(1\ 2\ 3) \circ (1\ 2)$ dh $1 \to 2 \& 2 \to 3$, also $1 \to 3$
$2 \to 1 \& 1 \to 2$, also $2 \to 2$
$3 \to 3 \& 3 \to 1$, also $3 \to 1$

Restklassen

Wiederholung:

Restklassen: Wir haben schon über Restklassen gesprochen und zwar als wir Äquivalenzklassen betrachtet haben

Wir erinnern uns:

$R_5 := \{(m, n) \subset \mathbb{Z} \times \mathbb{Z} | m - n \text{ ist ohne Rest durch 5 teilbar } \} \subset \mathbb{Z} \times \mathbb{Z}$

Wir haben dann die 5 Äquivalenzklassen
$[0] := \{0, 5, 10, 15, 20, \dots\}$
$[1] := \{1, 6, \dots\}$
$[2] := \{2, 7, \dots\}$
$[3] := \{3, 8, \dots\}$
$[4] := \{4, 9, \dots\}$
Man schreibt manchmal [5] statt [0] (man könnte auch [735] nehmen)

Restklassen

Man kann die Restklassen auch etwas anders aufschreiben:

$[1] := \{1, 6, \dots\} = 1 + 5 \cdot \mathbb{Z}$

Es hat sich eingebürgert dafür $\mathbb{Z}/n\mathbb{Z}$ zu schreiben und man kann auch Rechenoperationen darauf definieren:

Es gilt:

$$[a] + [b] := [a + b]$$
$$[a] \cdot [b] := [a \cdot b]$$

ZB $[2] + [4] = [2 + 4] = [6] = [1]$
oder $[5] \cdot [3] = [15] = [0] = [5]$

Restklassen

Es gilt: $(\mathbb{Z}/5\mathbb{Z}, +)$ ist eine Gruppe

(G0) $+$ ist eine Verknüpfung auf $\mathbb{Z}/5\mathbb{Z}$

(G1) $[0]$ ist das neutrale Element: $[a] + [0] = [a + 0] = [a]$

(G2) Für $[a]$ ist $[-a]$ das inverse Element: $[a] + [-a] = [a - a] = [0]$

(G3)
$[a]+([b]+[c]) = [a]+[b+c] = [a+b+c] = [a+b]+[c] = ([a]+[b])+[c]$

Restklassen

Exkurs:
Man müsste noch zeigen, dass die vorherige Definitionen **wohl-definiert** sind.
Wenn wir $[a] + [b]$ betrachten, dann ist die Frage, ob die Summe zweier Restklassen dadurch eindeutig bestimmt ist, oder vom Repräsentanten abhängt. Also: Macht es einen Unterschied, ob wir $[2] + [3]$ rechnen, oder $[12] + [13]$? Ist $[5] = [25]$?

Sei $[a_1] = [b_1]$ und $[a_2] = [b_2]$, dann muss gelten $[a_1 + a_2] = [b_1 + b_2]$.
Dies gilt, da $[a_1] = [b_1]$ bedeutet, dass sie modulo denselben Rest haben, also $a_1 = m_1 p + r_1$ und $b_1 = n_1 p + r_1$ mit $|r_1| < p$. Ebenso hält:
$a_2 = m_2 p + r_2$ und $b_2 = n_2 p + r_2$ mit $|r_2| < p$.
$\Rightarrow [a_1 + a_2] = [r_1 + r_2] = [b_1 + b_2]$

Restklassen

Anmerkung:
Auch ein Computer rechnet nur in Restklassen, wenn er addiert:
Nehmen wir an eine Zahl wird in einer 16-bit-Integer-Zahl gespeichert.
Eine solche Zahl kann dann maximal eine Größe von $65536 = 2^{16}$ haben.
Wenn wir zu 65536 noch $+1$ rechnen, dann findet ein Überlauf statt und die Zahl ist 0.
$\Rightarrow$ Restklasse $[65537]=[0]$

Ringe

Ringe

Definition:
Ein **Ring** $(R, \oplus, \odot)$ besteht aus einer Menge R mit zwei Verknüpfungen $\oplus$ und $\odot$ auf R mit den folgenden Eigenschaften:

(R1) $(R, \oplus)$ ist eine kommutative Gruppe.

(R2) Für alle $a, b, c \in R$ gilt: $a \odot (b \odot c) = (a \odot b) \odot c$.
(R ist *assoziativ*)

(R3) Für alle $a, b, c \in R$ gilt: $a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$.
Für alle $a, b, c \in R$ gilt: $(b \oplus c) \odot a = (b \odot a) \oplus (c \odot a)$.
(R ist *distributiv*)

Ringe

Definition:
Ein **Ring** $(R, \oplus, \odot)$ heißt außerdem **kommutativ**, wenn zusätzlich gilt:

(R4) Für alle $a, b \in R$ gilt $a \odot b = b \odot a$.

Ringe

Beispiele

Wir erinnern uns an $\mathbb{Z}/5\mathbb{Z}$ von dem wir gezeigt haben, dass $(\mathbb{Z}/5\mathbb{Z}, +)$ eine Gruppe ist. Man kann zeigen, dass $(\mathbb{Z}/5\mathbb{Z}, +, \cdot)$ sogar ein Ring ist:

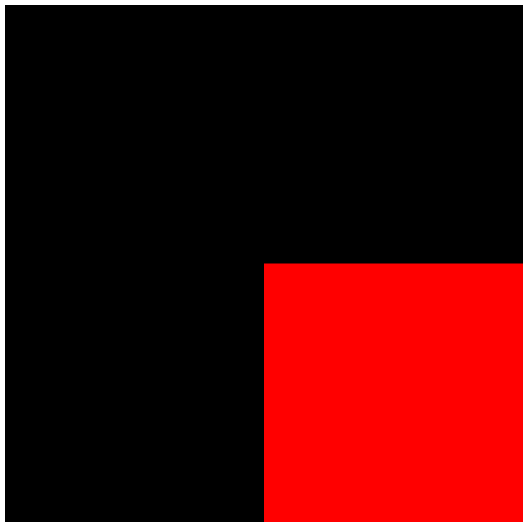
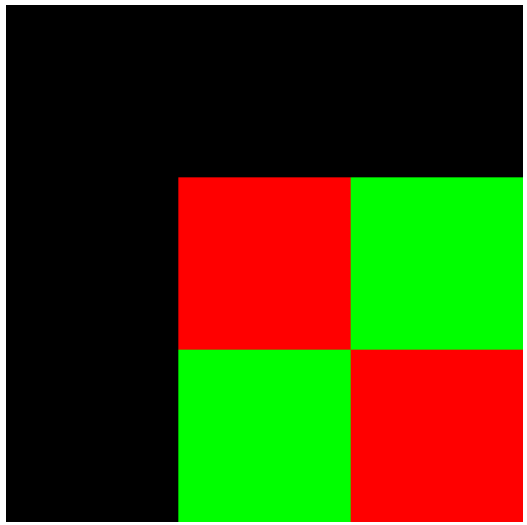
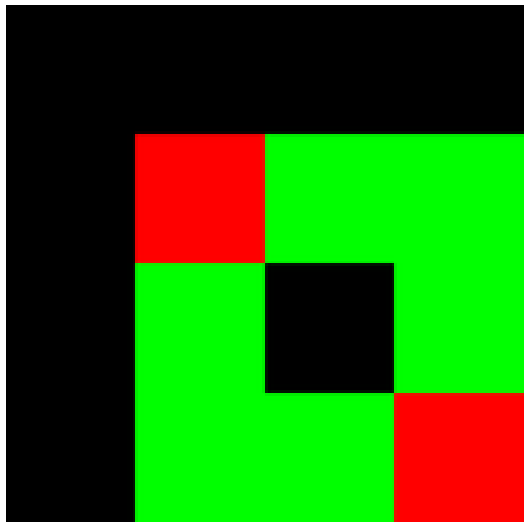
(R1) Wir müssen noch zeigen, dass $(\mathbb{Z}/5\mathbb{Z}, +)$ kommutativ ist, also $[a] + [b] = [b] + [a]$.
$[a] + [b] = [a + b] = [b + a] = [b] + [a]$

(R2) $[a] \cdot ([b] \cdot [c]) = [a] \cdot [b \cdot c] = [a \cdot b \cdot c] = [a \cdot b] \cdot [c] = ([a] \cdot [b]) \cdot [c]$.

(R3) Zu zeigen ist $[a] \cdot ([b] + [c]) = [a] \cdot [b] + [a] \cdot [c]$ und $([b] + [c]) \cdot [a] = [b] \cdot [a] + [c] \cdot [a]$.

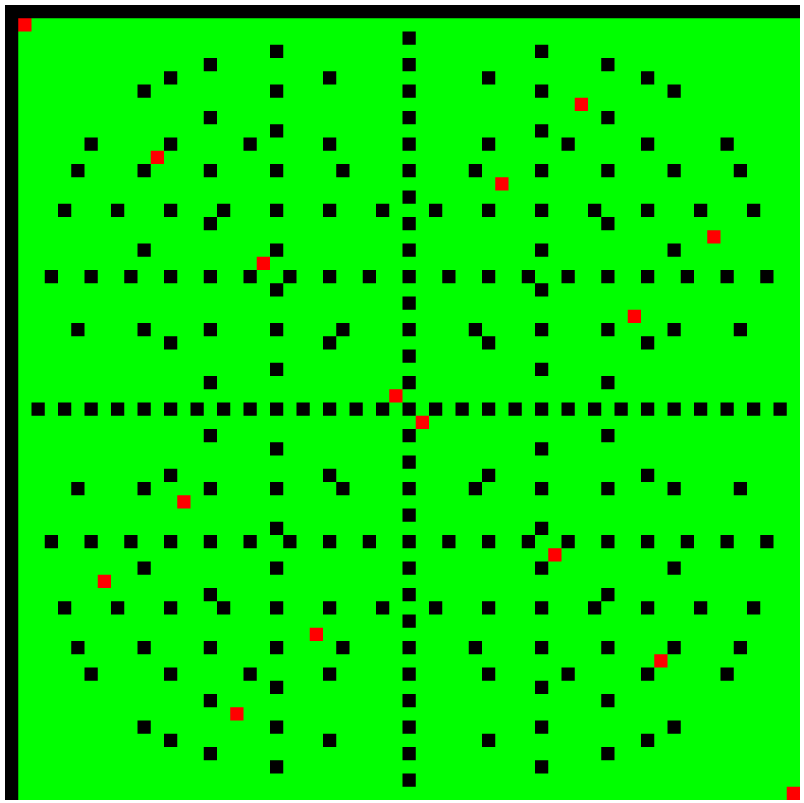
$\Rightarrow$ **Übungsaufgabe**

Ringe

Dies ist die Verknüpfungstafel bezüglich der Multiplikation von $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$ und $\mathbb{Z}/4\mathbb{Z}$. Schwarz ist [0] und rot [1]. Grün ist eine Restklasse, die weder [0] noch [1] ist.

Ringe



Das ist die Verknüpfungstafel für $\mathbb{Z}/60\mathbb{Z}$. Auch hier ist schwarz [0] und rot [1]. Grün ist eine Restklasse von [2]-[59].

Polynom-Ringe

Ein (für uns) besonders wichtiger Ring ist der **Polynomring** zu dem wir uns hinarbeiten:

Definition:
Sei R ein Ring mit $a_0, a_1, \ldots, a_n \in R$. Die Abbildung

$$f : R \to R, x \mapsto a_n x^n + a_{n-1} x^{n-1} + \ldots a_1 x + a_0$$

heißt **Polynom(funktion)** über R. Wenn $a_n \neq 0$ ist, ist n der **Grad** von f.

Ein Polynom ist eine altbekannte Sache, wenn man unter R $\mathbb{R}$ versteht, zB $f(x) = x + 1$ oder $f(x) = x^3 + 3 \cdot x^2 - 2$.

Polynom-Ringe

Ein Polynom macht aber (alleine) noch keinen Ring:

Definition:
Sei R ein Ring und wir bezeichnen die Menge aller Polynome über R mit $R[X]$. Wir haben die Verknüpfungen $+$ und $\cdot$ folgendermaßen definiert:

$$(1)\quad p + q = (p + q)(x) := p(x) + q(x)$$
$$(2)\quad p \cdot q = (p \cdot q)(x) := p(x) \cdot q(x)$$

$R[X]$ heißt dann **Polynomring** über R.

Körper

Körper

Definition:
Ein **Körper** $(K, \oplus, \odot)$ besteht aus einer Menge K und zwei Verknüpfungen $\oplus$ und $\odot$ auf K mit den folgenden Eigenschaften:

- (K1) $(K, \oplus, \odot)$ ist ein kommutativer Ring.
- (K2) Es gibt ein Element 1 in K mit $1 \odot a = a \odot 1 = a$ für alle $a \in K$ mit $a \neq 0$.
- (K3) Für alle $a \in K$ mit $a \neq 0$ gibt es ein Element $a^{-1} \in K$ mit $a^{-1} \odot a = 1$.

Es gilt also, dass $(K/\{0\}, \odot)$ eine Gruppe ist.

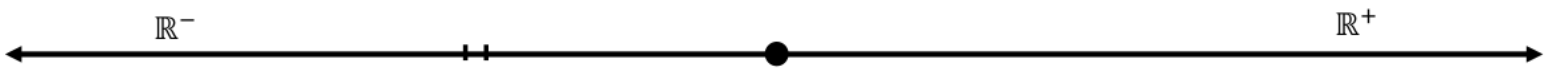
Körper

Definition in kurz:
Ein **Körper** $(K, \oplus, \odot)$ besteht aus einer Menge K und zwei Verknüpfungen $\oplus$ und $\odot$ auf K mit den folgenden Eigenschaften:

1) $(K, \oplus)$ ist eine abelsche Gruppe mit neutralem Element 0.
2) $(K/\{0\}, \odot)$ ist eine abelsche Gruppe mit neutralem Element 1.
3) $a \odot (b \oplus c) = a \odot b \oplus a \odot c$ und $(a \oplus b) \odot c = a \odot c \oplus b \odot c$ für alle $a, b, c \in K$.

Körper

Beispiele:
Körper sind für uns die wichtigsten Strukturen, da die „normale“ Auffassung von Zahlen dem eines Körpers, den reellen Zahlen $\mathbb{R}$, entspricht.



Als Informatiker muss man aber bedenken, dass man eigentlich „nur“ die rationalen Zahlen $\mathbb{Q}$ als Näherung zur Verfügung hat.
Sehr wichtig ist noch der Körper der komplexen Zahlen $\mathbb{C}$, der insbesondere für die Polynomdivision relevant ist, da er **algebraisch abgeschlossen** ist. Mehr dazu später.

Körper

Beispiel:
Ein Körper muss nicht unendlich groß sein: $\mathbb{F}_2$ etwa besteht nur aus den Elementen 0 und 1.

Die Verknüpfungen sind definiert als:

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

Ihr kennt $\mathbb{F}_2$ übrigens als $\mathbb{Z}/2\mathbb{Z}$.

Zusammenfassung

Gruppe $(G, *)$

- Verknüpfung $*$ auf Menge G assoziativ,
- neutrales Element e bzgl. $*$ vorhanden,
- $\forall a \in G$: inverses Element a^{-1} bzgl. $*$ vorhanden.
- optional: $*$ kommutativ (*abelsche Gruppe*)

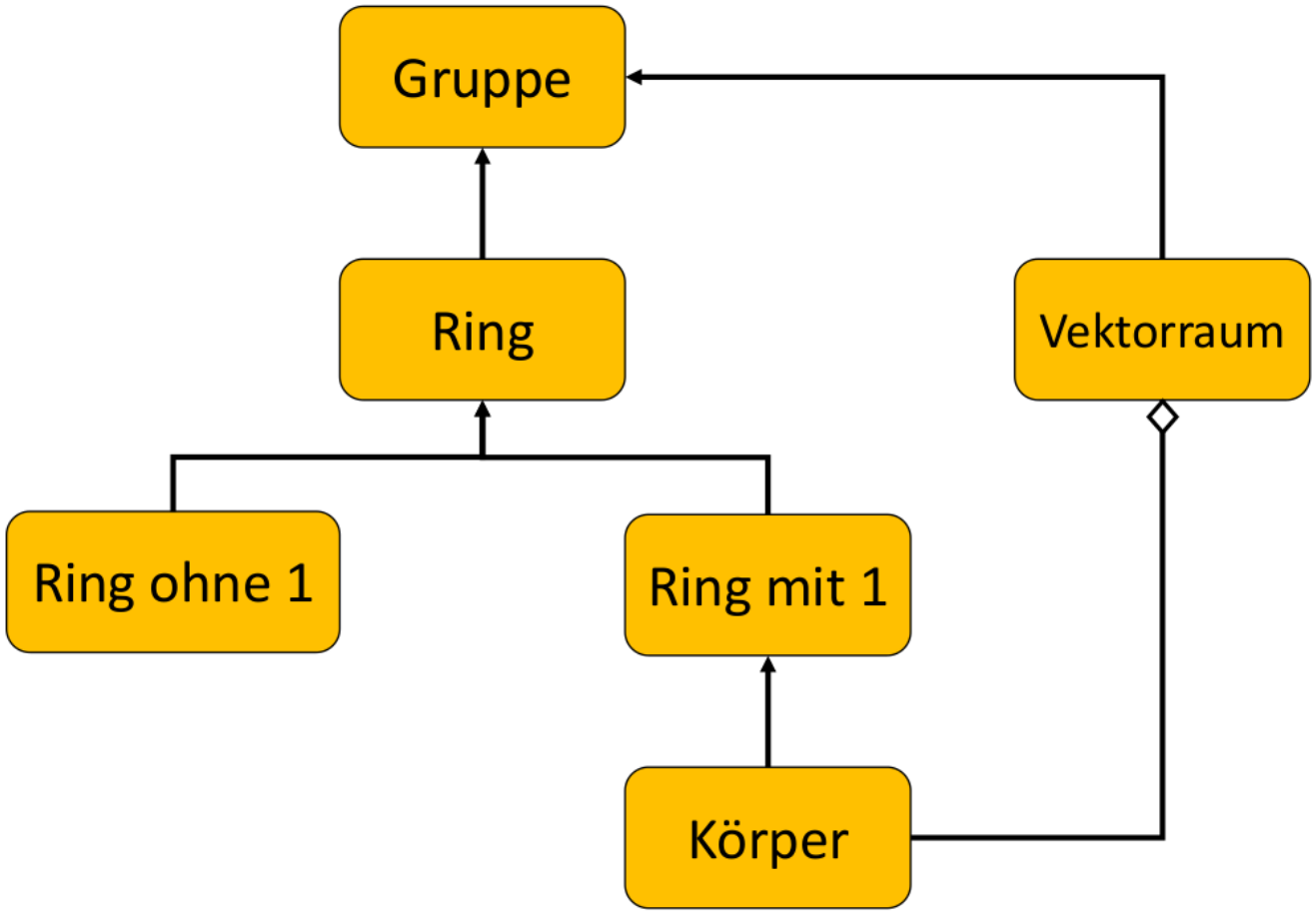
Ring $(R, \oplus, \odot)$

- $(R, \oplus)$ ist abelsche Gruppe,
- Verknüpfung $\odot$ assoziativ,
- Verknüpfungen $\oplus$ und $\odot$ distributiv,
- optional: $\odot$ kommutativ (*kommutativer Ring*), neutrales Element für $\odot$ (*Ring mit 1*)

Körper $(K, \oplus, \odot)$

- $(K, \oplus, \odot)$ ist kommutativer Ring,
- $(K, \oplus)$ ist abelsche Gruppe mit neutralem Element 0,
- $(K/\{0\}, \odot)$ ist abelsche Gruppe mit neutralem Element 1.

Übersicht über algebraische Strukturen



Anwendung: Public Key Verschlüsselungsverfahren

Mathematische Konzepte

- Ring $\mathbb{Z}/n\mathbb{Z}$,
- Abbildungen,
- Homomorphismen (in der nächsten Vorlesung).

Beispiel: RSA Algorithmus

benannt nach seinen Erfindern Rivest, Shamir und Adleman (1978).

Grundidee: 2 Schlüssel Jeder Teilnehmer besitzt 2 Schlüssel:

- **Public Key:** zum Verschlüsseln, für alle zugänglich
- **Private Key:** zum Entschlüsseln, geheim.

RSA

Grundidee: Wir brauchen eine Abbildung $f : O \to V, o \mapsto f(o)$, die jedem Originalzeichen $o \in O$ ein verschlüsseltes Zeichen $f(o) \in V$ zuordnet. f muss die folgenden Eigenschaften haben:

- f ist *bijektiv*,
- *Verschlüsseln einfach*: jeder kann $f(o)$ mit dem public key leicht berechnen,
- *Entschlüsseln einfach*: $f^{-1}(v)$ kann mit Hilfe des private keys leicht berechnet werden,
- *Angriff (fast) unmöglich*: $f^{-1}(v)$ kann ohne den private key nicht mit vertretbarem Aufwand berechnet werden.

RSA Algorithmus

Idee für Abbildung:

- Die Multiplikation von großen Primzahlen geht schnell und einfach, daher ein geeignetes $f(x)$.
- Die Zerlegung des Produkts in die Ausgangsfaktoren, d.h. die zugehörige Umkehrabbildung $f^{-1}(x)$ ist allerdings ohne Zusatzinformation sehr schwierig.

RSA Algorithmus

Algorithmus zur Schlüsselerzeugung:

1. Wähle zwei verschiedene große Primzahlen p und q,
2. Bilde daraus $n := pq$ (Produkt) und $m := (p-1)(q-1)$ ($\sharp$ teilerfremde Zahlen von n),
3. Wähle eine Zahl e, die teilerfremd zu m ist, z.B. eine Primzahl kleiner als m,
4. Berechne d als $e \cdot d \mod m = 1$, d.h. d ist das multiplikative Inverse von e
5. **Public Key**: (n, e), schicke ihn an alle anderen,
6. **Private Key**: (n, d), halte diesen geheim.

RSA

Verschlüsselung:
Wenn nun eine verschluesselte Nachricht verschickt wird so schlägt der Versender den **Public Key (n, e)** nach und verschlüsselt den Text wie folgt:

$$v = o^e \mod n$$

Dann wird der verschlüsselte Text verschickt.

RSA Algorithmus

Entschlüsselung:
Für die Entschlüsselung der verschlüsselten Nachricht braucht man dann den **Private Key (n, d)**:

$$o = v^d \mod n$$

Beispiel

Die Nachricht KLEOPATRA soll mit dem RSA Algorithmus verschluesselt werden.
public key (n, e) = (1147, 29)
Wir verschlüsseln nun jedes Zeichen:

$$v = o^{29} \mod 1147$$

o	10	11	4	14	15	0	19	17	0
v	803	730	132	547	277	0	979	42	0

Beispiel:

Die verschlüsselte Nachricht soll nun entschlüsselt werden.
Public Key $(n, e) = (1147, 29)$
Private Key $(n, d) = (1147, 149)$
Wie sieht die Funktion aus mit der wir aus v o wiederherstellen können?

$$o = v^{149} \mod 1147$$

Und was passiert wenn wir diese Funktion auf die v Werte der verschlüsselten Nachricht anwenden?
Wenn wir nun die v Werte in die Formel einsetzen erhalten wir die originalen o Werte (10, 11, 4, ...) wieder.

Wie kann man die Verschlüsselung brechen?

Um den Private Key (n, d) aus dem Public Key (n, e) zu ermitteln sind folgende Schritte nötig:

$$ed = 1 \mod m$$

Um m zu erhalten müsste man zuerst die Primfaktoren von p und q von n bestimmen, denn $m = (p-1)(q-1)$. Dies wird schnell sehr komplex vor allem wenn n groß ist.

Beispiel:

In unserem Beispiel ist die Primfaktorenzerlegung allerdings möglich, da n zu klein

Wie müsste man vorgehen?

1. Man muesste n vom public key in seine Primfaktoren zerlegen

$$1147 = 31 \cdot 37$$

2. Damit kann man m berechnen

$$\text{m} = (31\text{-}1)(37\text{-}1) = 1080$$

3. Da nun m und e bekannt sind kann d einfach berechnet werden (Euklidscher Algorithmus für ggT).

Wie sicher ist RSA?

- **Heute:** gute Sicherheit. Typische Größe für n: 2048 Bit (das ist eine Zahl mit 617 Stellen im Dezimalsystem).
- **Zukunft:** Quantencomputer werden das Problem in viel kürzerer (polynomieller) Zeit lösen können, daher brauchen wir andere Verschlüsselungstechniken.

Literatur

- Einführung RSA `http://www.mathematik.de/ger/information/wasistmathematik/rsa/rsa.html`
- Euklidscher Algorithmus `http://www.mathematik.de/ger/information/wasistmathematik/rsa/rsa_euklid.html`
- Algorithmen für Primfaktorzerlegung `www.mit.edu/~yongwhan/projects/math249b.pdf`
- Verschlüsselung in der Zukunft `https://www.quantamagazine.org/20150908-quantum-safe-encryption/`
- Xinming Huang, Wei Wang: A Novel and Efficient Design for an RSA Cryptosystem With a Very Large Key Size. IEEE Trans. on Circuits and Systems 62-II(10): 972-976 (2015)