# Vorkurs
# Formale Methoden der Informatik

Bettina Esser und Michael Kaibel

2. September bis 13. September 2024, Universität Bonn

Informatik V

# Die algebraische Hierarchie

# Magma $\rightarrow$ Halbgruppe

**Definition**

Sei $(M, \circ)$ ein Magma. Erinnerung: Eine Menge $M$ zusammen mit einer zweistelligen abgeschlossenen Verknüpfung $\circ$.

# Magma $\rightarrow$ Halbgruppe

**Definition**

Sei $(M, \circ)$ ein Magma. Erinnerung: Eine Menge $M$ zusammen mit einer zweistelligen abgeschlossenen Verknüpfung $\circ$.

$(M, \circ)$ heißt Halbgruppe, wenn zusätzlich das Assoziativgesetz gilt, d.h. $x \circ (y \circ z) = (x \circ y) \circ z$ für alle $x, y, z \in M$.

# Magma $\rightarrow$ Halbgruppe

**Definition**

Sei $(M, \circ)$ ein Magma. Erinnerung: Eine Menge $M$ zusammen mit einer zweistelligen abgeschlossenen Verknüpfung $\circ$.

$(M, \circ)$ heißt Halbgruppe, wenn zusätzlich das Assoziativgesetz gilt, d.h. $x \circ (y \circ z) = (x \circ y) \circ z$ für alle $x, y, z \in M$.

**Beispiel**

- $(\mathbb{N}, \circ)$ mit $n \circ m = \max(n, m)$ ist eine Halbgruppe, da die Maximumsfunktion assoziativ ist.

# Magma $\rightarrow$ Halbgruppe

**Definition**

Sei $(M, \circ)$ ein Magma. Erinnerung: Eine Menge $M$ zusammen mit einer zweistelligen abgeschlossenen Verknüpfung $\circ$.

$(M, \circ)$ heißt Halbgruppe, wenn zusätzlich das Assoziativgesetz gilt, d.h. $x \circ (y \circ z) = (x \circ y) \circ z$ für alle $x, y, z \in M$.

**Beispiel**

- $(\mathbb{N}, \circ)$ mit $n \circ m = \max(n, m)$ ist eine Halbgruppe, da die Maximumsfunktion assoziativ ist.
- $(\mathbb{R}, \circ)$ mit $x \circ y = x - y$ ist keine Halbgruppe, da $\circ$ nicht assoziativ ist.

# Halbgruppe $\rightarrow$ Monoid

**Definition**

Sei $(M, \circ)$ eine Halbgruppe.

# Halbgruppe $\rightarrow$ Monoid

**Definition**

Sei $(M, \circ)$ eine Halbgruppe.

$(M, \circ)$ heißt Monoid, wenn zusätzlich ein neutrales Element existiert, d.h. es existiert ein $e \in M$ sodass $x \circ e = e \circ x = x$ für alle $x \in M$.

# Halbgruppe $\rightarrow$ Monoid

**Definition**

Sei $(M, \circ)$ eine Halbgruppe.

$(M, \circ)$ heißt Monoid, wenn zusätzlich ein neutrales Element existiert, d.h. es existiert ein $e \in M$ sodass $x \circ e = e \circ x = x$ für alle $x \in M$.Gilt für $(M, \circ)$ das Kommutativgesetz, nennen wir $M$ einen kommutativen Monoid.

# Halbgruppe $\rightarrow$ Monoid

## Definition

Sei $(M, \circ)$ eine Halbgruppe.

$(M, \circ)$ heißt Monoid, wenn zusätzlich ein neutrales Element existiert, d.h. es existiert ein $e \in M$ sodass $x \circ e = e \circ x = x$ für alle $x \in M$.Gilt für $(M, \circ)$ das Kommutativgesetz, nennen wir $M$ einen kommutativen Monoid.

## Beispiel

- $(\mathbb{N}, \circ)$ mit $n \circ m = \max(n, m)$ ist ein Monoid mit neutralem Element $1$, da für alle $x \in \mathbb{N}$ gilt: $\max(n, 1) = n$, da $n \geq 1$.

# Halbgruppe $\rightarrow$ Monoid

## Definition

Sei $(M, \circ)$ eine Halbgruppe.

$(M, \circ)$ heißt Monoid, wenn zusätzlich ein neutrales Element existiert, d.h. es existiert ein $e \in M$ sodass $x \circ e = e \circ x = x$ für alle $x \in M$.Gilt für $(M, \circ)$ das Kommutativgesetz, nennen wir $M$ einen kommutativen Monoid.

## Beispiel

- $(\mathbb{N}, \circ)$ mit $n \circ m = \max(n, m)$ ist ein Monoid mit neutralem Element $1$, da für alle $x \in \mathbb{N}$ gilt: $\max(n, 1) = n$, da $n \geq 1$.
- $(\mathbb{Z}, \circ)$ mit $n \circ m = \max(n, m)$ ist kein Monoid, da $\mathbb{Z}$ kein kleinstes Element, damit $\max$ kein neutrales Element besitzt.

# Halbgruppe $\rightarrow$ Monoid

## Definition

Sei $(M, \circ)$ eine Halbgruppe.

$(M, \circ)$ heißt Monoid, wenn zusätzlich ein neutrales Element existiert, d.h. es existiert ein $e \in M$ sodass $x \circ e = e \circ x = x$ für alle $x \in M$.Gilt für $(M, \circ)$ das Kommutativgesetz, nennen wir $M$ einen kommutativen Monoid.

## Beispiel

- $(\mathbb{N}, \circ)$ mit $n \circ m = \max(n, m)$ ist ein Monoid mit neutralem Element $1$, da für alle $x \in \mathbb{N}$ gilt: $\max(n, 1) = n$, da $n \geq 1$.
- $(\mathbb{Z}, \circ)$ mit $n \circ m = \max(n, m)$ ist kein Monoid, da $\mathbb{Z}$ kein kleinstes Element, damit $\max$ kein neutrales Element besitzt.
- $(\mathcal{P}(X), \bigcap)$ ist ein Monoid für jede Menge $X$ (Übung).

# Halbgruppe $\rightarrow$ Monoid

## Definition

Sei $(M, \circ)$ eine Halbgruppe.

$(M, \circ)$ heißt Monoid, wenn zusätzlich ein neutrales Element existiert, d.h. es existiert ein $e \in M$ sodass $x \circ e = e \circ x = x$ für alle $x \in M$.Gilt für $(M, \circ)$ das Kommutativgesetz, nennen wir $M$ einen kommutativen Monoid.

## Beispiel

- $(\mathbb{N}, \circ)$ mit $n \circ m = \max(n, m)$ ist ein Monoid mit neutralem Element $1$, da für alle $x \in \mathbb{N}$ gilt: $\max(n, 1) = n$, da $n \geq 1$.
- $(\mathbb{Z}, \circ)$ mit $n \circ m = \max(n, m)$ ist kein Monoid, da $\mathbb{Z}$ kein kleinstes Element, damit $\max$ kein neutrales Element besitzt.
- $(\mathcal{P}(X), \bigcap)$ ist ein Monoid für jede Menge $X$ (Übung).
- $(\mathcal{P}(X), \bigcup)$ ebenfalls (Übung).

# Monoid $\rightarrow$ Gruppe

**Definition**

Sei $(M, \circ)$ ein Monoid mit neutralem Element $e$.

# Monoid $\rightarrow$ Gruppe

**Definition**

Sei $(M, \circ)$ ein Monoid mit neutralem Element $e$.

Dann heißt $(M, \circ)$ eine Gruppe, wenn zusätzlich $M$ ein inverse Elemente besitzt, d.h. für jedes $x \in M$ existiert ein $y \in M$ mit $x \circ y = y \circ x = e$.

# Monoid $\rightarrow$ Gruppe

**Definition**

Sei $(M, \circ)$ ein Monoid mit neutralem Element $e$.

Dann heißt $(M, \circ)$ eine Gruppe, wenn zusätzlich $M$ ein inverse Elemente besitzt, d.h. für jedes $x \in M$ existiert ein $y \in M$ mit $x \circ y = y \circ x = e$.

**Beispiel**

- Alles, was wir gestern kennengelernt haben.

# Gruppe $\rightarrow$ Abelsche Gruppe

**Definition**

Sei $(G, \circ)$ eine Gruppe.

**Definition**

Sei $(G, \circ)$ eine Gruppe.

Gilt zusätzlich das Kommutativgesetz, d.h. für alle $x, y \in G$ gilt $x \circ y = y \circ x$, so nennen wir $G$ abelsch.

# Gruppe $\rightarrow$ Abelsche Gruppe

**Definition**

Sei $(G, \circ)$ eine Gruppe.

Gilt zusätzlich das Kommutativgesetz, d.h. für alle $x, y \in G$ gilt $x \circ y = y \circ x$, so nennen wir $G$ abelsch.

**Beispiel**

- Alle zyklischen Gruppen $C_n$ sind abelsch.

# Gruppe $\rightarrow$ Abelsche Gruppe

**Definition**

Sei $(G, \circ)$ eine Gruppe.

Gilt zusätzlich das Kommutativgesetz, d.h. für alle $x, y \in G$ gilt $x \circ y = y \circ x$, so nennen wir $G$ abelsch.

**Beispiel**

- Alle zyklischen Gruppen $C_n$ sind abelsch.
- Die Kleinsche Vierergruppe $K_4$ ist abelsch.

# Gruppe $\rightarrow$ Abelsche Gruppe

**Definition**

Sei $(G, \circ)$ eine Gruppe.

Gilt zusätzlich das Kommutativgesetz, d.h. für alle $x, y \in G$ gilt $x \circ y = y \circ x$, so nennen wir $G$ abelsch.

**Beispiel**

- Alle zyklischen Gruppen $C_n$ sind abelsch.
- Die Kleinsche Vierergruppe $K_4$ ist abelsch.
- Die Diedergruppen $D_n$ sind im allgemeinen nicht abelsch.

# Abelsche Gruppe $\rightarrow$ Ring

**Definition**

Sei $(R, +, \cdot)$ eine Menge mit zwei Verknüpfungen $+, \cdot$.

# Abelsche Gruppe $\rightarrow$ Ring

**Definition**

Sei $(R, +, \cdot)$ eine Menge mit zwei Verknüpfungen $+, \cdot$.Dann heißt $R$ Ring wenn folgende Regeln gelten:

# Abelsche Gruppe $\rightarrow$ Ring

**Definition**

Sei $(R, +, \cdot)$ eine Menge mit zwei Verknüpfungen $+, \cdot$.Dann heißt $R$ Ring wenn folgende Regeln gelten:

- $(R, +)$ ist eine abelsche Gruppe. Wir benennen das neutrale Element bzgl. $+$ mit $e_+ = 0$.

# Abelsche Gruppe $\rightarrow$ Ring

**Definition**

Sei $(R, +, \cdot)$ eine Menge mit zwei Verknüpfungen $+, \cdot$.Dann heißt $R$ Ring wenn folgende Regeln gelten:

- $(R, +)$ ist eine abelsche Gruppe. Wir benennen das neutrale Element bzgl. $+$ mit $e_+ = 0$.
- $(R, \cdot)$ ist eine Halbgruppe.

# Abelsche Gruppe $\rightarrow$ Ring

**Definition**

Sei $(R, +, \cdot)$ eine Menge mit zwei Verknüpfungen $+, \cdot$.Dann heißt $R$ Ring wenn folgende Regeln gelten:

- $(R, +)$ ist eine abelsche Gruppe. Wir benennen das neutrale Element bzgl. $+$ mit $e_+ = 0$.
- $(R, \cdot)$ ist eine Halbgruppe.
- Es gilt das Distributivgesetz: Für alle $a, b, c \in R$ gilt: $a \cdot (b + c) = a \cdot b + a \cdot c$

# Abelsche Gruppe $\rightarrow$ Ring

**Definition**

Sei $(R, +, \cdot)$ eine Menge mit zwei Verknüpfungen $+, \cdot$.Dann heißt $R$ Ring wenn folgende Regeln gelten:

- $(R, +)$ ist eine abelsche Gruppe. Wir benennen das neutrale Element bzgl. $+$ mit $e_+ = 0$.
- $(R, \cdot)$ ist eine Halbgruppe.
- Es gilt das Distributivgesetz: Für alle $a, b, c \in R$ gilt: $a \cdot (b + c) = a \cdot b + a \cdot c$

Manchmal wollen wir zusätzliche Eigenschaften für $\cdot$ fordern

- ist $(R, \cdot)$ zusätzlich kommutativ, so ist $R$ ein kommutativer Ring
- Ist $R, \cdot$ ein Monoid, so ist $R$ ein Ring mit $1$. Wir nennen das neutrale Element der Multiplikation $1$, $e. = 1$
- Ist $R$ kommutativ und mit $1$, so ist $R$ ein kommutativer Ring mit $1$

# Beispiele für Ringe

**Beispiel**

- $(\mathbb{Z}, +, \cdot), (\mathbb{Q}, +, \cdot)$ und $(\mathbb{R}, +, \cdot)$ sind prototypische kommutative Ringe mit $1$.

# Beispiele für Ringe

**Beispiel**

- $(\mathbb{Z}, +, \cdot), (\mathbb{Q}, +, \cdot)$ und $(\mathbb{R}, +, \cdot)$ sind prototypische kommutative Ringe mit $1$.
- $(\{0, \ldots, n-1\}, +\mod n, \cdot \mod n) = \mathbb{Z}_n$ sind ebenfalls kommutative Ringe mit $1$. Sie sind wichtige Ringe in der Kryptographie und augenscheinlich eng verwandt mit den zyklischen Gruppen $C_n$.

# Beispiele für Ringe

**Beispiel**

- $(\mathbb{Z}, +, \cdot), (\mathbb{Q}, +, \cdot)$ und $(\mathbb{R}, +, \cdot)$ sind prototypische kommutative Ringe mit $1$.
- $(\{0, \ldots, n-1\}, +\mod n, \cdot \mod n) = \mathbb{Z}_n$ sind ebenfalls kommutative Ringe mit $1$. Sie sind wichtige Ringe in der Kryptographie und augenscheinlich eng verwandt mit den zyklischen Gruppen $C_n$.
- $(\mathbb{R}[X], +, \cdot)$, der kommutative Ring mit $1$ aller Polynome mit reellen Koeffizienten und normaler Addition/Multiplikation ist ein zentraler Ring in der abstrakten Algebra.

# Beispiele für Ringe

**Beispiel**

- $(\mathbb{Z}, +, \cdot), (\mathbb{Q}, +, \cdot)$ und $(\mathbb{R}, +, \cdot)$ sind prototypische kommutative Ringe mit $1$.
- $(\{0, \ldots, n-1\}, +\mod n, \cdot \mod n) = \mathbb{Z}_n$ sind ebenfalls kommutative Ringe mit $1$. Sie sind wichtige Ringe in der Kryptographie und augenscheinlich eng verwandt mit den zyklischen Gruppen $C_n$.
- $(\mathbb{R}[X], +, \cdot)$, der kommutative Ring mit $1$ aller Polynome mit reellen Koeffizienten und normaler Addition/Multiplikation ist ein zentraler Ring in der abstrakten Algebra.
- $(\mathbb{R}^{n \times n}, +, \cdot)$ mit $n \geq 2$ und $+, \cdot$ als Matrixaddition/multiplikation ist ein wichtiger Ring mit $1$, aber nicht kommututativ. Er hat große Bedeutung in linearer Algebra.

# Beispiele für Ringe

**Beispiel**

- $(\mathbb{Z}, +, \cdot), (\mathbb{Q}, +, \cdot)$ und $(\mathbb{R}, +, \cdot)$ sind prototypische kommutative Ringe mit $1$.
- $(\{0, \ldots, n-1\}, +\mod n, \cdot \mod n) = \mathbb{Z}_n$ sind ebenfalls kommutative Ringe mit $1$. Sie sind wichtige Ringe in der Kryptographie und augenscheinlich eng verwandt mit den zyklischen Gruppen $C_n$.
- $(\mathbb{R}[X], +, \cdot)$, der kommutative Ring mit $1$ aller Polynome mit reellen Koeffizienten und normaler Addition/Multiplikation ist ein zentraler Ring in der abstrakten Algebra.
- $(\mathbb{R}^{n\times n}, +, \cdot)$ mit $n \geq 2$ und $+, \cdot$ als Matrixaddition/multiplikation ist ein wichtiger Ring mit $1$, aber nicht kommututativ. Er hat große Bedeutung in linearer Algebra.
- Ringe die weder kommutativ sind, noch eine $1$ haben, sind meistens nicht interessant. Ein Beispiel ist $(\{..., -4, -2, 0, -2, -4, ...\}^{n\times n}, +, *)$ der Ring aller Matrizen mit geraden ganzzahligen Einträgen.

# Ring $\rightarrow$ Integritätsbereich

**Definition**

Sei $(R, +, \cdot)$ ein kommutativer Ring mit $1$.

# Ring $\rightarrow$ Integritätsbereich

**Definition**

Sei $(R, +, \cdot)$ ein kommutativer Ring mit $1$.

$(R, +, \cdot)$ heißt Integritätsbereich, wenn die Eigenschaft der Nullteilerfreiheit erfüllt ist:

# Ring $\rightarrow$ Integritätsbereich

**Definition**

Sei $(R, +, \cdot)$ ein kommutativer Ring mit $1$.

$(R, +, \cdot)$ heißt Integritätsbereich, wenn die Eigenschaft der Nullteilerfreiheit erfüllt ist:

Für alle $a, b \in R$ gilt: $a \cdot b = 0 \Rightarrow (a = 0 \vee b = 0)$. Wörtlich: $0$ besitzt keine echten Teiler außer der $0$.

# Ring $\rightarrow$ Integritätsbereich

## Definition

Sei $(R, +, \cdot)$ ein kommutativer Ring mit $1$.

$(R, +, \cdot)$ heißt Integritätsbereich, wenn die Eigenschaft der Nullteilerfreiheit erfüllt ist:

Für alle $a, b \in R$ gilt: $a \cdot b = 0 \Rightarrow (a = 0 \vee b = 0)$. Wörtlich: $0$ besitzt keine echten Teiler außer der $0$.

Zudem muss $0 \neq 1$ erfüllt sein. Wörtlich: Das neutrale Element von $+$ und das neutrale Element von $\cdot$ dürfen nicht gleich sein.

## Beispiel

- $Z_6$ ist kein Integritätsbereich, da hier $2 \cdot 3 = 0$ gilt.
- $Z_7$ ist ein Integritätsbereich.
- $(\mathbb{R}, +, \cdot)$ ist ein Integritätsbereich.
- $Z_n$ ist ein Integritätsbereich genau dann, wenn $n$ eine Primzahl ist. (Übung)

# Die Kürzungsregel

**Theorem**

*Sei* $(R, +, \cdot)$ *ein Integritätsbereich, gelte* $a \cdot b = a \cdot c$ *für* $a, b, c \in R, a \neq 0$. *Dann gilt* $b = c$.

# Die Kürzungsregel

**Theorem**

*Sei* $(R, +, \cdot)$ *ein Integritätsbereich, gelte* $a \cdot b = a \cdot c$ *für* $a, b, c \in R, a \neq 0$. *Dann gilt* $b = c$.

**Beweis.**

Beweis durch Umformungen:

# Die Kürzungsregel

**Theorem**

*Sei* $(R, +, \cdot)$ *ein Integritätsbereich, gelte* $a \cdot b = a \cdot c$ *für* $a, b, c \in R, a \neq 0$. *Dann gilt* $b = c$.

**Beweis.**

Beweis durch Umformungen:

$$
\begin{aligned}
& a \cdot b = a \cdot c \\
\iff\ & a \cdot b + -(a \cdot c) = 0 \\
\iff\ & a \cdot b + a \cdot (-c) = 0 \\
\iff\ & a \cdot (b + (-c)) = 0 \\
\Rightarrow\ & a = 0 \vee (b + (-c)) = 0 \\
\Rightarrow\ & (b + (-c)) = 0 \\
\iff\ & b = c.
\end{aligned}
$$

□

# Ring $\rightarrow$ Körper

**Definition**

Sei $(R, +, \cdot)$ ein Ring.

# Ring $\rightarrow$ Körper

**Definition**

Sei $(R, +, \cdot)$ ein Ring.

Gilt zusätzlich, dass $(R \setminus \{0\}, \cdot)$ eine abelsche Gruppe ist, dann heißt $(R, +, \cdot)$ ein Körper.

# Ring $\rightarrow$ Körper

**Definition**

Sei $(R, +, \cdot)$ ein Ring.

Gilt zusätzlich, dass $(R \setminus \{0\}, \cdot)$ eine abelsche Gruppe ist, dann heißt $(R, +, \cdot)$ ein Körper.

Ein Körper ist auch immer ein Ring mit $1$, da $(R \setminus \{0\}, \cdot)$ in einem Körper kommutativ ist und uns ein $1$-Element gibt. Die $0$ noch hinzuzufügen zerstört uns weder die kommutativität, noch die $1$, da $0 \cdot x = 0 = x \cdot 0$ gilt (Übung zu zeigen).

**Beispiel**

- $(\mathbb{Q}, +, \cdot)$ und $(\mathbb{R}, +, \cdot)$ sind Körper.

# Ring $\rightarrow$ Körper

**Definition**

Sei $(R, +, \cdot)$ ein Ring.

Gilt zusätzlich, dass $(R \setminus \{0\}, \cdot)$ eine abelsche Gruppe ist, dann heißt $(R, +, \cdot)$ ein Körper.

Ein Körper ist auch immer ein Ring mit $1$, da $(R \setminus \{0\}, \cdot)$ in einem Körper kommutativ ist und uns ein $1$-Element gibt. Die $0$ noch hinzuzufügen zerstört uns weder die kommutativität, noch die $1$, da $0 \cdot x = 0 = x \cdot 0$ gilt (Übung zu zeigen).

**Beispiel**

- $(\mathbb{Q}, +, \cdot)$ und $(\mathbb{R}, +, \cdot)$ sind Körper.
- $(\mathbb{Z}, +, \cdot)$ ist kein Körper (z.B. $2$ besitzt kein multiplikatives Inverses).

# Ring $\rightarrow$ Körper

**Definition**

Sei $(R, +, \cdot)$ ein Ring.

Gilt zusätzlich, dass $(R \setminus \{0\}, \cdot)$ eine abelsche Gruppe ist, dann heißt $(R, +, \cdot)$ ein Körper.

Ein Körper ist auch immer ein Ring mit $1$, da $(R \setminus \{0\}, \cdot)$ in einem Körper kommutativ ist und uns ein $1$-Element gibt. Die $0$ noch hinzuzufügen zerstört uns weder die kommutativität, noch die $1$, da $0 \cdot x = 0 = x \cdot 0$ gilt (Übung zu zeigen).

**Beispiel**

- $(\mathbb{Q}, +, \cdot)$ und $(\mathbb{R}, +, \cdot)$ sind Körper.
- $(\mathbb{Z}, +, \cdot)$ ist kein Körper (z.B. $2$ besitzt kein multiplikatives Inverses).
- $(Z_n, +, \cdot)$ ist genau dann ein Körper, wenn $n$ eine Primzahl ist. (Korollar nächster Folie)

# Der noch kleinere Satz von Wedderburn

**Theorem (Miniversion vom „Kleinen Satz von Wedderburn")**

*Jeder endliche Integritätsbereich ist ein Körper.*

# Der noch kleinere Satz von Wedderburn

**Theorem (Miniversion vom „Kleinen Satz von Wedderburn")**

*Jeder endliche Integritätsbereich ist ein Körper.*

**Beweis.**

Sei $(R, +, \cdot)$ ein endlicher Integritätsbereich. Es bleibt nach Definition zu zeigen, dass $R \setminus \{0\}$ multiplikative Inverse besitzt, d.h. dass für jedes $x \in R$ mit $x \neq 0$ ein $y \in R$ existiert mit $x \cdot y = 1$.

# Der noch kleinere Satz von Wedderburn

**Theorem (Miniversion vom „Kleinen Satz von Wedderburn")**

*Jeder endliche Integritätsbereich ist ein Körper.*

**Beweis.**

Sei $(R, +, \cdot)$ ein endlicher Integritätsbereich. Es bleibt nach Definition zu zeigen, dass $R \setminus \{0\}$ multiplikative Inverse besitzt, d.h. dass für jedes $x \in R$ mit $x \neq 0$ ein $y \in R$ existiert mit $x \cdot y = 1$.

Sei $n = |R|$, und sei ein beliebiges $x \in R$ mit $x \neq 0$ gegeben. Betrachte die Potenzen von $x$: $x^1, x^2, \ldots, x^{n+1}$.

# Der noch kleinere Satz von Wedderburn

**Theorem (Miniversion vom „Kleinen Satz von Wedderburn")**

*Jeder endliche Integritätsbereich ist ein Körper.*

**Beweis.**

Sei $(R, +, \cdot)$ ein endlicher Integritätsbereich. Es bleibt nach Definition zu zeigen, dass $R \setminus \{0\}$ multiplikative Inverse besitzt, d.h. dass für jedes $x \in R$ mit $x \neq 0$ ein $y \in R$ existiert mit $x \cdot y = 1$.

Sei $n = |R|$, und sei ein beliebiges $x \in R$ mit $x \neq 0$ gegeben. Betrachte die Potenzen von $x$: $x^1, x^2, \ldots, x^{n+1}$. Da $R$ nur $n$ Elemente hat, muss es nach dem Schubfachprinzip $k$ und $i$ (o.B.d.A $k > i$) geben mit $x^k = x^i$.

# Der noch kleinere Satz von Wedderburn

**Theorem (Miniversion vom „Kleinen Satz von Wedderburn")**

*Jeder endliche Integritätsbereich ist ein Körper.*

**Beweis.**

Sei $(R, +, \cdot)$ ein endlicher Integritätsbereich. Es bleibt nach Definition zu zeigen, dass $R \setminus \{0\}$ multiplikative Inverse besitzt, d.h. dass für jedes $x \in R$ mit $x \neq 0$ ein $y \in R$ existiert mit $x \cdot y = 1$.

Sei $n = |R|$, und sei ein beliebiges $x \in R$ mit $x \neq 0$ gegeben. Betrachte die Potenzen von $x$: $x^1, x^2, \ldots, x^{n+1}$. Da $R$ nur $n$ Elemente hat, muss es nach dem Schubfachprinzip $k$ und $i$ (o.B.d.A $k > i$) geben mit $x^k = x^i$.

Schreibe $x^k$ als $x^i \cdot x^{k-i}$, $x^i$ als $x^i \cdot 1$.

# Der noch kleinere Satz von Wedderburn

**Theorem (Miniversion vom „Kleinen Satz von Wedderburn")**

*Jeder endliche Integritätsbereich ist ein Körper.*

**Beweis.**

Sei $(R, +, \cdot)$ ein endlicher Integritätsbereich. Es bleibt nach Definition zu zeigen, dass $R \setminus \{0\}$ multiplikative Inverse besitzt, d.h. dass für jedes $x \in R$ mit $x \neq 0$ ein $y \in R$ existiert mit $x \cdot y = 1$.

Sei $n = |R|$, und sei ein beliebiges $x \in R$ mit $x \neq 0$ gegeben. Betrachte die Potenzen von $x$: $x^1, x^2, \ldots, x^{n+1}$. Da $R$ nur $n$ Elemente hat, muss es nach dem Schubfachprinzip $k$ und $i$ (o.B.d.A $k > i$) geben mit $x^k = x^i$.

Schreibe $x^k$ als $x^i \cdot x^{k-i}$, $x^i$ als $x^i \cdot 1$. Es gilt also $x^i \cdot x^{k-i} = x^i \cdot 1$.

# Der noch kleinere Satz von Wedderburn

**Theorem (Miniversion vom „Kleinen Satz von Wedderburn")**

*Jeder endliche Integritätsbereich ist ein Körper.*

**Beweis.**

Sei $(R, +, \cdot)$ ein endlicher Integritätsbereich. Es bleibt nach Definition zu zeigen, dass $R \setminus \{0\}$ multiplikative Inverse besitzt, d.h. dass für jedes $x \in R$ mit $x \neq 0$ ein $y \in R$ existiert mit $x \cdot y = 1$.

Sei $n = |R|$, und sei ein beliebiges $x \in R$ mit $x \neq 0$ gegeben. Betrachte die Potenzen von $x$: $x^1, x^2, \ldots, x^{n+1}$. Da $R$ nur $n$ Elemente hat, muss es nach dem Schubfachprinzip $k$ und $i$ (o.B.d.A $k > i$) geben mit $x^k = x^i$.

Schreibe $x^k$ als $x^i \cdot x^{k-i}$, $x^i$ als $x^i \cdot 1$. Es gilt also $x^i \cdot x^{k-i} = x^i \cdot 1$. Nach der Kürzungsregel für Integritätsbereiche gilt $x^{k-i} = 1$.

# Der noch kleinere Satz von Wedderburn

**Theorem (Miniversion vom „Kleinen Satz von Wedderburn")**

*Jeder endliche Integritätsbereich ist ein Körper.*

**Beweis.**

Sei $(R, +, \cdot)$ ein endlicher Integritätsbereich. Es bleibt nach Definition zu zeigen, dass $R \setminus \{0\}$ multiplikative Inverse besitzt, d.h. dass für jedes $x \in R$ mit $x \neq 0$ ein $y \in R$ existiert mit $x \cdot y = 1$.

Sei $n = |R|$, und sei ein beliebiges $x \in R$ mit $x \neq 0$ gegeben. Betrachte die Potenzen von $x$: $x^1, x^2, \ldots, x^{n+1}$. Da $R$ nur $n$ Elemente hat, muss es nach dem Schubfachprinzip $k$ und $i$ (o.B.d.A $k > i$) geben mit $x^k = x^i$.

Schreibe $x^k$ als $x^i \cdot x^{k-i}$, $x^i$ als $x^i \cdot 1$. Es gilt also $x^i \cdot x^{k-i} = x^i \cdot 1$. Nach der Kürzungsregel für Integritätsbereiche gilt $x^{k-i} = 1$. Das bedeutet aber nur, dass $x^{k-i-1} \cdot x = 1$, also ist $x$ invertierbar. □