Wieso Körper?

Mit Ringen haben wir etwas analoges zu $\mathbb{Z}$ oder $\mathbb{Z}_n$ gefunden. Wir können addieren, subtrahieren, multiplizieren und bekommen Eigenschaften wie

Wieso Körper?

Mit Ringen haben wir etwas analoges zu $\mathbb{Z}$ oder $\mathbb{Z}_n$ gefunden. Wir können addieren, subtrahieren, multiplizieren und bekommen Eigenschaften wie

- $0a = 0$

Wieso Körper?

Mit Ringen haben wir etwas analoges zu $\mathbb{Z}$ oder $\mathbb{Z}_n$ gefunden. Wir können addieren, subtrahieren, multiplizieren und bekommen Eigenschaften wie

- $0a = 0$
- $(-1)b = -b$

Wieso Körper?

Mit Ringen haben wir etwas analoges zu $\mathbb{Z}$ oder $\mathbb{Z}_n$ gefunden. Wir können addieren, subtrahieren, multiplizieren und bekommen Eigenschaften wie

- $0a = 0$
- $(-1)b = -b$
- $(-a)(-b) = ab$

Wieso Körper?

Mit Ringen haben wir etwas analoges zu $\mathbb{Z}$ oder $\mathbb{Z}_n$ gefunden. Wir können addieren, subtrahieren, multiplizieren und bekommen Eigenschaften wie

- $0a = 0$
- $(-1)b = -b$
- $(-a)(-b) = ab$
- $a + b = b \implies a = 0$

Wieso Körper?

Mit Ringen haben wir etwas analoges zu $\mathbb{Z}$ oder $\mathbb{Z}_n$ gefunden. Wir können addieren, subtrahieren, multiplizieren und bekommen Eigenschaften wie

- $0a = 0$
- $(-1)b = -b$
- $(-a)(-b) = ab$
- $a + b = b \implies a = 0$

Aber viele wichtige Eigenschaften und Operationen wie in $\mathbb{R}$ oder $\mathbb{Q}$ haben wir nicht:

Wieso Körper?

Mit Ringen haben wir etwas analoges zu $\mathbb{Z}$ oder $\mathbb{Z}_n$ gefunden. Wir können addieren, subtrahieren, multiplizieren und bekommen Eigenschaften wie

- $0a = 0$
- $(-1)b = -b$
- $(-a)(-b) = ab$
- $a + b = b \implies a = 0$

Aber viele wichtige Eigenschaften und Operationen wie in $\mathbb{R}$ oder $\mathbb{Q}$ haben wir nicht:

- Wir können nicht dividieren (angenommen $a \neq 0$):

$$ax = b \implies x = \frac{b}{a}$$

Wieso Körper?

Mit Ringen haben wir etwas analoges zu $\mathbb{Z}$ oder $\mathbb{Z}_n$ gefunden. Wir können addieren, subtrahieren, multiplizieren und bekommen Eigenschaften wie

- $0a = 0$
- $(-1)b = -b$
- $(-a)(-b) = ab$
- $a + b = b \implies a = 0$

Aber viele wichtige Eigenschaften und Operationen wie in $\mathbb{R}$ oder $\mathbb{Q}$ haben wir nicht:

- Wir können nicht dividieren (angenommen $a \neq 0$):

$$ax = b \implies x = \frac{b}{a}$$

- $a \cdot b = 0 \implies a = 0$ oder $b = 0$ (gilt nur in einem "integral domain")

Wieso Körper?

Mit Ringen haben wir etwas analoges zu $\mathbb{Z}$ oder $\mathbb{Z}_n$ gefunden. Wir können addieren, subtrahieren, multiplizieren und bekommen Eigenschaften wie

- $0a = 0$
- $(-1)b = -b$
- $(-a)(-b) = ab$
- $a + b = b \implies a = 0$

Aber viele wichtige Eigenschaften und Operationen wie in $\mathbb{R}$ oder $\mathbb{Q}$ haben wir nicht:

- Wir können nicht dividieren (angenommen $a \neq 0$):

$$ax = b \implies x = \frac{b}{a}$$

- $a \cdot b = 0 \implies a = 0$ oder $b = 0$ (gilt nur in einem "integral domain")
- $\deg(p(x) \cdot q(x)) = \deg(p(x)) + \deg(q(x))$

Daher:

Definition (5.26.)

Ein Körper F ist ein nichttrivialer kommutativer Ring mit $F^* = F \setminus \{0\}$. (Das heisst, jedes Element ausser 0 hat ein Inverses bezüglich Multiplikation.)

Daher:

Definition (5.26.)

Ein Körper F ist ein nichttrivialer kommutativer Ring mit $F^* = F \setminus \{0\}$. (Das heisst, jedes Element ausser 0 hat ein Inverses bezüglich Multiplikation.)

Anders gesagt ist $\langle F \setminus \{0\}; \cdot, ^{-1}, 1 \rangle$ eine Gruppe.

Daher:

Definition (5.26.)

Ein Körper F ist ein nichttrivialer kommutativer Ring mit $F^* = F \setminus \{0\}$. (Das heisst, jedes Element ausser 0 hat ein Inverses bezüglich Multiplikation.)

Anders gesagt ist $\langle F \setminus \{0\}; \cdot, ^{-1}, 1\rangle$ eine Gruppe.

Invertierbarkeit von 0 verlangen wir nicht, aus dem gleichen Grund, wieso $\frac{1}{0}$ nicht definiert ist.

Polynome über einem Körper

Die Polynome $F[x]$ haben viele Eigenschaften, die uns an $\mathbb{Z}$ erinnern.

Polynome über einem Körper

Die Polynome $F[x]$ haben viele Eigenschaften, die uns an $\mathbb{Z}$ erinnern.
In $\mathbb{Z}$ können wir für jedes $a, m \in \mathbb{Z}$, a als

$$a = m \cdot q + r, \quad r = R_m(a)$$
$$17 = 3 \cdot 5 + 2$$

schreiben.

Polynome über einem Körper

Die Polynome $F[x]$ haben viele Eigenschaften, die uns an $\mathbb{Z}$ erinnern.
In $\mathbb{Z}$ können wir für jedes $a, m \in \mathbb{Z}$, a als

$$a = m \cdot q + r, \quad r = R_m(a)$$
$$17 = 3 \cdot 5 + 2$$

schreiben.
Genauso wie wir in $\mathbb{Z}$ über Reste sprechen können, können wir dies auch in $F[x]$ tun!

Satz (5.25.)

Für jedes $a(x), m(x) \in F[x]$ gibt es $q(x), r(x)$, so dass

$$a(x) = m(x) \cdot q(x) + r(x), \quad r(x) = R_{m(x)}(a(x))$$

und

$$\deg(r(x)) < \deg(m(x)) \quad \textit{(analog zu } r < |m| \textit{ in } \mathbb{Z}\textit{)}$$

Polynomdivision in $\mathbb{Z}_p$

Teile $x^4 + 3x^2 + 4$ durch $4x^2 + 2x + 1$ in $\mathbb{Z}_5$ mit Rest.

Mithile vom letzten Satz sehen wir, dass wir mit einem beliebigen Polynom $m(x)$ den Rest Modulo $m(x)$ betrachten können.

Mithile vom letzten Satz sehen wir, dass wir mit einem beliebigen Polynom $m(x)$ den Rest Modulo $m(x)$ betrachten können.
Analog also wie $\mathbb{Z}_m$ können wir folgenden Ring definieren

Definition (5.35.)

$$F[x]_{m(x)} = \{a(x) \in F[x] \mid \deg(a(x)) < \deg(m(x))\}$$

Das sind alle möglichen Reste Modulo $m(x)$.

Modulo Arithmetik mit Polynomen

Berechne

$$(x+3)(x+2)$$

in $\mathbb{Z}_5[x]_{x^2+4}$

Irreduzible Polynome

Genauso wie wir in $\mathbb{Z}$ Primzahlen haben, haben wir in $F[x]$ *irreduzible* Polynome.

Irreduzible Polynome

Genauso wie wir in $\mathbb{Z}$ Primzahlen haben, haben wir in $F[x]$ *irreduzible* Polynome.

Definition (5.28.)

Ein Polynom $a(x) \in F[x]$ heisst *irreduzibel*, wenn es keinen Teiler $m(x)$ hat mit $0 < \deg(m(x)) < \deg(a(x))$ (analog dazu, dass eine Primzahl keine Teiler zwischen 1 und p hat).

Irreduzible Polynome

Genauso wie wir in $\mathbb{Z}$ Primzahlen haben, haben wir in $F[x]$ *irreduzible* Polynome.

Definition (5.28.)

Ein Polynom $a(x) \in F[x]$ heisst *irreduzibel*, wenn es keinen Teiler $m(x)$ hat mit $0 < \deg(m(x)) < \deg(a(x))$ (analog dazu, dass eine Primzahl keine Teiler zwischen 1 und p hat).

Und analog wie in $\mathbb{Z}$ kann auch jedes Polynom $a(x) \in F[x]$ in irreduzible Polynome faktorisiert werden.

Folgende Tatsache, der uns von Polynomen über $\mathbb{R}$ bekannt ist, hilft uns, Irreduzibilität zu überprüfen.

Folgende Tatsache, der uns von Polynomen über $\mathbb{R}$ bekannt ist, hilft uns, Irreduzibilität zu überprüfen.

Lemma (5.29.)

$\alpha \in F$ ist eine Nullstelle von $a(x) \iff (x - \alpha) \mid a(x)$.

Irreduzibilität überprüfen

Strategie um Teiler von $a(x)$ zu finden:

1. Überprüfe, ob $a(x)$ Nullstellen hat.
2. Überprüfe für alle **irreduziblen** Polynome mit Grad $1 < d \leq \deg(a(x))/2$, ob sie $a(x)$ teilen.

Irreduzibilität überprüfen

Strategie um Teiler von $a(x)$ zu finden:

1. Überprüfe, ob $a(x)$ Nullstellen hat.
2. Überprüfe für alle **irreduziblen** Polynome mit Grad $1 < d \leq \deg(a(x))/2$, ob sie $a(x)$ teilen.

Sind die folgenden Polynome irreduzibel? Wenn nicht, dann faktorisiere sie

Irreduzibilität überprüfen

Strategie um Teiler von $a(x)$ zu finden:

1. Überprüfe, ob $a(x)$ Nullstellen hat.
2. Überprüfe für alle **irreduziblen** Polynome mit Grad $1 < d \leq \deg(a(x))/2$, ob sie $a(x)$ teilen.

Sind die folgenden Polynome irreduzibel? Wenn nicht, dann faktorisiere sie

- $x^2 + 4$ in $\mathbb{Z}_5$

Irreduzibilität überprüfen

Strategie um Teiler von $a(x)$ zu finden:

1. Überprüfe, ob $a(x)$ Nullstellen hat.
2. Überprüfe für alle **irreduziblen** Polynome mit Grad $1 < d \leq \deg(a(x))/2$, ob sie $a(x)$ teilen.

Sind die folgenden Polynome irreduzibel? Wenn nicht, dann faktorisiere sie

- $x^2 + 4$ in $\mathbb{Z}_5$
- $x^3 + 2x^2 + 1$ in $\mathbb{Z}_3$

Irreduzibilität überprüfen

Strategie um Teiler von $a(x)$ zu finden:

1. Überprüfe, ob $a(x)$ Nullstellen hat.
2. Überprüfe für alle **irreduziblen** Polynome mit Grad $1 < d \leq \deg(a(x))/2$, ob sie $a(x)$ teilen.

Sind die folgenden Polynome irreduzibel? Wenn nicht, dann faktorisiere sie

- $x^2 + 4$ in $\mathbb{Z}_5$
- $x^3 + 2x^2 + 1$ in $\mathbb{Z}_3$
- $x^4 + x^2 + 1$ in $\mathbb{Z}_2$
  Hinweis: $x^2 + x + 1$ ist das einzige irreduzible Polynom in $\mathbb{Z}_2$ von Grad 2.

Modulo und Teilbarkeit kombiniert

In $\mathbb{Z}$ haben wir gesehen:

Lemma (4.18.)

$$ax \equiv_m 1$$

ist lösbar für $x \in \mathbb{Z}_m$ genau dann, wenn $\gcd(a, m) = 1$.

Modulo und Teilbarkeit kombiniert

In $\mathbb{Z}$ haben wir gesehen:

Lemma (4.18.)

$$ax \equiv_m 1$$

ist lösbar für $x \in \mathbb{Z}_m$ *genau dann, wenn* $\gcd(a, m) = 1$.

Auch dazu haben wir auch ein Analogon:

Lemma (5.36.)

$$a(x)b(x) \equiv_{m(x)} 1$$

hat eine Lösung $b(x) \in F[x]$ *genau dann, wenn* $\gcd(a(x), m(x)) = 1$.

Und wir können genauso von der multiplikativen Gruppe modulo $m(x)$ sprechen (vergleiche $\mathbb{Z}_m^*$)

Lemma (5.36.)

$$F[x]^*_{m(x)} = \left\{a(x) \in F[x]_{m(x)} \mid \gcd(a(x), m(x)) = 1\right\}$$

Der Ring $\mathbb{Z}_p[x]_{m(x)}$

Betrachte den Ring $\mathbb{Z}_3[x]_{x^2+2}$.

Der Ring $\mathbb{Z}_p[x]_{m(x)}$

Betrachte den Ring $\mathbb{Z}_3[x]_{x^2+2}$.

1. Bestimme alle Nullteiler von $\mathbb{Z}_3[x]_{x^2+2}$.

Der Ring $\mathbb{Z}_p[x]_{m(x)}$

Betrachte den Ring $\mathbb{Z}_3[x]_{x^2+2}$.

1. Bestimme alle Nullteiler von $\mathbb{Z}_3[x]_{x^2+2}$.
2. Liste alle Elemente der Gruppe $\mathbb{Z}_3[x]^*_{x^2+2}$ auf.

Der Ring $\mathbb{Z}_p[x]_{m(x)}$

Betrachte den Ring $\mathbb{Z}_3[x]_{x^2+2}$.

1. Bestimme alle Nullteiler von $\mathbb{Z}_3[x]_{x^2+2}$.
2. Liste alle Elemente der Gruppe $\mathbb{Z}_3[x]^*_{x^2+2}$ auf.
3. Bestimme das Inverse von $2x$ in der Gruppe $\mathbb{Z}_3[x]^*_{x^2+2}$.

“Verschachtelte” Polynome

Ist das Polynom $xy^3 + xy^2 + (x+1)y + x \in \mathbb{Z}_2[x]_{x^2+x+1}[y]$ irreduzibel?