Übersicht
Vorlesungswoche 2

Ulrich Görtz

Lineare Algebra 2, SS 21

Erinnerung

R Ring

R $\quad + : R \times R \to R$, $\quad \cdot : R \times R \to R$

Ringhomomorphismen, Ringisomorphismen

Ideale $\quad \mathfrak{a} \subseteq R$ $\quad$ { Untergruppe bzgl $+$; für alle $x \in R$, $a \in \mathfrak{a}$ gilt $xa \in \mathfrak{a}$, $ax \in \mathfrak{a}$ }

Polynomring

R kommutativ

$$R[X] = \left\{ \sum_{i=0}^{n} a_i X^i \; ; \; n \in \mathbb{N}, \; a_i \in R \right\}$$

Integritätsringe

R kommutativer Ring

R Integritätsring $\iff$

- $R \neq \{0\}$
- für alle $x, y \in R \setminus \{0\}$ gilt

$$x y \neq 0.$$

Teilbarkeit

R Integritätsbereich, $a, b \in R$

$a \mid b \iff$ es ex. $c \in R$: $b = ca$.

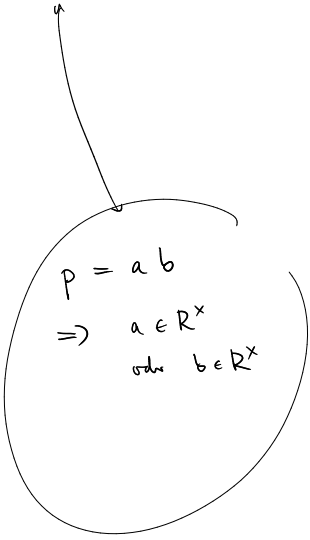
Euklidische Ringe und Hauptidealringe

R Integritätsbereich

In R existiert
"Division mit Rest"

für jedes Ideal $\mathfrak{a} \subseteq R$
ex. $a \in R$ mit $\mathfrak{a} = (a)$.

Irreduzible und prime Elemente



R Integritätsbereich

$p \in R$, $p \notin R^\times$
$p \neq 0$

"Primelementeigenschaft"

$p \mid ab \Rightarrow p \mid a$ oder $p \mid b$.

Integritätsringe
Vorlesungswoche 2

Ulrich Görtz

Lineare Algebra 2, SS 21

UNIVERSITÄT
DUISBURG
ESSEN

Definition Integritätsring

Def. Ein kommutativer Ring R heißt Integritätsring, wenn $R \neq 0$ und für alle $x, y \in R$ mit $xy = 0$ gilt: $x = 0$ oder $y = 0$.

Quiz

Welche der folgenden Ringe sind Integritätsringe?

$\mathbb{Z}$

K ein Körper

Für welche n ist $\mathbb{Z}/n$ ein Integritätsring?

Finden Sie Ringe R
- einerseits, so dass $\mathrm{Pol}(R)$ ein Integritätsring ist,
- andererseits, so dass $\mathrm{Pol}(R)$ kein Integritätsring ist.

Quiz

Welche der folgenden Ringe sind Integritätsringe?

$\mathbb{Z}$ ist ein Integritätsring

K ein Körper — Jeder Körper ist ein Integritätsring.

n keine Primzahl $\rightsquigarrow$ $n = ab$, $1 < a, b < n$ $\rightsquigarrow$ $a \cdot b = 0$ in $\mathbb{Z}/n$, $a, b \neq 0$

Für welche n ist $\mathbb{Z}/n$ ein Integritätsring? — $\mathbb{Z}/n$ Integritätsring $\Leftrightarrow$ n Primzahl ($n \in \mathbb{N}_{>0}$)

Finden Sie Ringe R

- einerseits, so dass $\mathrm{Pol}(R)$ ein Integritätsring ist, — z.B. $R = \mathbb{Q}$ (allgemeiner z.B. für jeden unendlichen Körper R)
- andererseits, so dass $\mathrm{Pol}(R)$ kein Integritätsring ist. — z.B. $R = \mathbb{F}_2$ (allgemeiner: R endl. Kp)

Die Kürzungsregel

R Integritätsring

Sind $a, b, c \in R$ mit $a \neq 0$ und $ab = ac$,

dann folgt $b = c$.

(Denn $ab = ac \Rightarrow a(b-c) = 0$

$\Rightarrow$ $a = 0$ oder $b - c = 0$).

ausgeschlossen

Grad von Summe und Produkt von Polynomen

R kommutativer Ring, $R[X] = \left\{ \sum_{i=0}^{n} a_i X^i \right\} \ni f = \sum_{i=0}^{n} a_i X^i$, $a_n \neq 0$

$\rightsquigarrow \quad \deg(f) = n$

(und $\deg(0) := -\infty$)

Lemma Seien $f, g \in R[X]$.

(1) $\deg(f+g) \leq \max(\deg(f), \deg(g))$

(2) $\deg(fg) \leq \deg(f) + \deg(g)$ und wenn R Integritätsring, dann gilt "$=$".

Beweis (2) Sei $f = \sum_{i=0}^{m} a_i X^i$, $g = \sum_{i=0}^{n} b_i X^i$ mit $m = \deg f$, $n = \deg g$

Dann gilt $f \cdot g = \sum_{i=0}^{m+n} \left(\sum_{j+k=i} a_j b_k \right) X^i$, [falls $f \neq 0$, $g \neq 0$]

und so folgt $\deg(f \cdot g) \leq m+n$.

Der Koeffizient von X^{m+n} im Produkt fg ist $a_m b_n$.

Ist $m = \deg f$, $n = \deg g$, dann heißt das $a_m \neq 0$, $b_n \neq 0$.

Wenn R Integritätsring, dann folgt $a_m b_n \neq 0$, also

$$\deg(fg) = m+n.$$

Sonderfall: $f = 0$ (oder $g = 0$). Dann ist $fg = 0$ und

"$-\infty + \deg(g) = -\infty$"

Polynomringe über Integritätsringen

Korollar Sei R ein Integritätsring. Dann ist auch $R[X]$ ein Integritätsring.
Es gilt $R[X]^\times = R^\times$.

Beweis Seien $f, g \in R[X] \setminus \{0\}$. Dann gilt $\deg(f), \deg(g) \in \mathbb{N}$.
Es folgt $\deg(fg) = \deg(f) + \deg(g) \in \mathbb{N}$, also $\deg(fg) \neq -\infty$.
Das bedeutet $fg \neq 0$. (Außerdem $R[X] \neq 0$, weil $R \neq 0$.)

Außerdem ist offenbar $R^\times \subseteq R[X]^\times$. Ist $f \in R[X]^\times$, dann
existiert $g \in R[X]$ mit $fg = 1$. Es folgt $0 = \deg(1) = \deg(fg)$
$= \deg(f) + \deg(g)$.

Deshalb ist $\deg(f) = \deg(g) = 0$, also $f, g \in R^\times$.

Teilbarkeit in Integritätsringen
Vorlesungswoche 2

Ulrich Görtz

Lineare Algebra 2, SS 21

UNIVERSITÄT
DUISBURG
ESSEN

Definition: Teilbar, Teiler, Vielfaches, Assoziiertheit

R Integritätsring (d.h. $R \neq 0$, und $xy = 0 \Rightarrow x = 0$ oder $y = 0$
$\rightsquigarrow ab = ac,\ a \neq 0 \Rightarrow b = c$)

Definition Seien $a, b \in R$.

(1) Wir sagen a sei ein Teiler von b (oder: b sei ein Vielfaches von a), wenn $c \in R$ existiert mit $b = c \cdot a$. Wir schreiben dann $a \mid b$. (Andernfalls: $a \nmid b$)

(2) Die Elemente a und b heißen assoziiert zueinander, wenn $c \in R^\times$ existiert, s.d. $b = c \cdot a$ (also $a = c^{-1} \cdot b$).

Teilbarkeit und Ideale

R Integritätsring, $a, b \in R$

Lemma (1) $a \mid b \iff b \in (a) \iff (b) \subseteq (a)$

$\| \quad \{ca \,;\, c \in R\}$

(2) a, b assoziiert zueinander $\iff a \mid b$ und $b \mid a \overset{(1)}{\iff} (a) = (b)$

Beweis zu (2) Wenn a, b zueinander assoziiert sind, so folgt direkt $a \mid b$, $b \mid a$.

Gelte nun $a \mid b$ und $b \mid a$, etwa $b = ca$, $a = db$, $c, d \in R$.

Dann $b = ca = cdb$, also $(1 - cd)\, b = 0$

R Integritätsring $\rightsquigarrow$ $b = 0$ (dann $a = db = 0$, also $a = 0$)

oder $1 - cd = 0$, d.h. $cd = 1$, wobei $c \in R^\times$.

Quiz

In welchen der folgenden Fälle gilt $a \mid b$ im Ring R?

$R = \mathbb{Z}$, $a = 2$, $b = 4$.

$R = \mathbb{Z}$, $a = 2$, $b = 3$.

$R = \mathbb{Z}$, $a = 2$, $b = -2$.

$R = \mathbb{Q}$, $a = 2$, $b = 3$.

$R = \mathbb{C}[X]$, $a = iX - 1$, $b = X^2 + 1$

Quiz

In welchen der folgenden Fälle gilt $a \mid b$ im Ring R?

$R = \mathbb{Z}$, $a = 2$, $b = 4$. $2 \mid 4$, denn $4 = 2 \cdot 2$

$R = \mathbb{Z}$, $a = 2$, $b = 3$. $2 \nmid 3$, denn es gibt kein $c \in \mathbb{Z}$ mit $3 = c \cdot 2$

$R = \mathbb{Z}$, $a = 2$, $b = -2$. $2 \mid -2$, denn $-2 = (-1) \cdot 2$

$R = \mathbb{Q}$, $a = 2$, $b = 3$. $2 \mid 3$, denn $3 = \frac{3}{2} \cdot 2$

$R = \mathbb{C}[X]$, $a = iX - 1$, $b = X^2 + 1$ $(iX - 1) \mid (X^2 + 1)$, denn $X^2 + 1 = (-iX - 1)(iX - 1)$

Quiz

Wann sind Elemente zueinander assoziiert

- im Ring $\mathbb{Z}$?

- in einem Körper K?

- im Ring $\mathbb{Q}[X]$?

Quiz

Wann sind Elemente zueinander assoziiert

- im Ring $\mathbb{Z}$? $a, b \in \mathbb{Z}$ zueinander assoz. $\iff$ $a = b$ oder $a = -b$

- in einem Körper K? $a, b \in K$ zueinander assoz. $\iff$ $a, b \neq 0$ oder $a = b = 0$.

- im Ring $\mathbb{Q}[X]$? $f, g \in \mathbb{Q}[X]$ zueinander assoziiert $\iff$ es ex. $c \in \mathbb{Q}^\times$ mit $g = c \cdot f$.

$\mathbb{Q}[X]^\times = \mathbb{Q}^\times$

Euklidische Ringe
Vorlesungswoche 2

Ulrich Görtz

Lineare Algebra 2, SS 21

Essen Seminar for Algebraic Geometry and Arithmetic

UNIVERSITÄT DUISBURG ESSEN

Erinnerung: Division mit Rest in $\mathbb{Z}$

Satz Seien $a, b \in \mathbb{Z}$, $b \neq 0$. Dann existieren ganze Zahlen q und r, so dass

$$a = b \cdot q + r \quad \text{und} \quad 0 \leq r < |b|.$$

„Division von a durch b ergibt q, Rest r."

Quiz

Schreiben Sie $f = X^4 + 3X^2 + 2X + 1 \in \mathbb{R}[X]$ in der Form $q \cdot (X^2 - X) + r$ mit $\deg(r) < 2$.

Quiz

Schreiben Sie $f = X^4 + 3X^2 + 2X + 1 \in \mathbb{R}[X]$ in der Form $q \cdot (X^2 - X) + r$ mit $\deg(r) < 2$.

$$X^4 + 3X^2 + 2X + 1 = (X^2 - X) \cdot \underbrace{(X^2 + X + 4)}_{q} + \underbrace{(6X + 1)}_{r}$$

$$\begin{array}{r} X^4 + 3X^2 + 2X + 1 \\ -(X^4 - X^3) \\ \hline X^3 + 3X^2 + 2X + 1 \\ -(X^3 - X^2) \\ \hline 4X^2 + 2X + 1 \\ -(4X^2 - 4X) \\ \hline 6X + 1 \end{array}$$

Polynomdivision

Satz Sei R ein Integritätsring, seien $f, g \in R[X]$, so dass Leitkoeff. von g in $R^\times$ (insbes. $g \neq 0$). Dann existieren $q, r \in R[X]$ mit $f = q \cdot g + r$ und $r = 0$ oder $\deg(r) < \deg(g)$

Beweis durch Induktion nach $\deg(f)$. IA Falls $\deg(f) < \deg(g)$, dann können wir $q := 0$, $r := f$ setzen.

IS. Sei nun $\underbrace{\deg f}_{m} \geq \underbrace{\deg g}_{n}$ (insbes. $f \neq 0$).

Seien a bzw. b die Leitkoeffizienten von f bzw. g.

$f = aX^m + \dots$

$g = bX^n + \dots$

$(b \in R^\times)$

Sei $h := f - ab^{-1}X^{m-n}g$

Dann $\deg(h) < \deg(f)$. Nach IV ex. $q_1, r \in R[X]$

Polynomdivision

mit $h = q_1 \cdot g + r, \quad \deg(r) < \deg(g)$

Es gilt dann $f = h + ab^{-1} X^{m-n} g$

$= q_1 g + r + ab^{-1} X^{m-n} g$

$= \underbrace{(q_1 + ab^{-1} X^{m-n})}_{=: q} g + r, \quad \deg(r) < \deg(g).$

Bem. Ist $R = K$ ein Körper, so können wir für g im Satz über die Polynomdiv. jedes Polynom $\neq 0$ verwenden.

Euklidische Ringe

Def. Ein Integritätsring R heißt euklidischer Ring, wenn eine Abbildung

$$\delta : R \setminus \{0\} \longrightarrow \mathbb{N}$$ (eine sogenannte Gradabbildung),

so dass für alle $a, b \in R$, $b \neq 0$, Elemente $q, r \in R$ existieren mit $a = q \cdot b + r$, und

- $r = 0$, oder
- $r \neq 0$ und $\delta(r) < \delta(b)$.

Beispiele

- $\mathbb{Z}$ ist euklidisch (Gradabb.: $\mathbb{Z} \setminus \{0\} \to \mathbb{N}$, $a \mapsto |a|$)

- K Körper $\Rightarrow$ $K[X]$ euklidisch,
  (Gradabb. $K[X] \setminus \{0\} \to \mathbb{N}$, $f \mapsto \deg(f)$)

Hauptidealringe
Vorlesungswoche 2

Ulrich Görtz

Lineare Algebra 2, SS 21

UNIVERSITÄT
DUISBURG
ESSEN

Hauptideale, Hauptidealringe

Def. (1) Sei R ein Ring. Ein Ideal $\mathfrak{a} \subseteq R$ heißt *Hauptideal*, wenn $a \in R$ existiert mit $\mathfrak{a} = (a)$.

R kommutativ:
$(a) = \{ra;\ r \in R\}$

(2) Ein R heißt *Hauptidealring*, wenn R ein Integritätsring ist, so dass jedes Ideal von R ein Hauptideal ist.

Euklidische Ringe sind Hauptidealringe

Satz Sei R ein euklidischer Ring. Dann ist R ein Hauptidealring.

Beweis Sei $\delta : R \setminus \{0\} \to \mathbb{N}$ eine Gradabbildung.

Sei $\mathfrak{a} \subseteq R$ ein Ideal. Ist $\mathfrak{a} = \{0\}$, dann ist $\mathfrak{a} = (0)$ ein Hauptideal.

Sei nun $\mathfrak{a} \neq 0$, und sei $a \in \mathfrak{a} \setminus \{0\}$, so dass $\delta(a)$ minimal ist unter allen Werten von δ auf Elem. von $\mathfrak{a} \setminus \{0\}$.

Beh. $\mathfrak{a} = (a)$. **Begr.** "$\supseteq$" klar, denn $a \in \mathfrak{a}$.

"$\subseteq$" Sei $x \in \mathfrak{a}$. Schreibe $x = qa + r$, $q, r \in R$, $r = 0$ oder $r \neq 0$ und $\delta(r) < \delta(a)$.

1. Fall $r = 0$, dann $x = qa \in (a)$.

2. Fall $r \neq 0$. Dann gilt $\delta(r) < \delta(a)$ und $r = x - qa \in \mathfrak{a}$ – Widerspruch zur Wahl von a

Beispiele für Hauptidealringe

- $\mathbb{Z}$
- $K[X]$ für K Körper.

Quiz

Finden Sie einen Erzeuger

des Ideals $(6, 15, 27)$ in $\mathbb{Z}$

des Ideals $(X^p - 1,\ p \text{ Primzahl}) = (X^2 - 1, X^3 - 1, X^5 - 1, \dots)$ in $\mathbb{C}[X]$

Quiz

Finden Sie einen Erzeuger

$(6, 15, 27) = (3)$ $\subseteq$ $6, 15, 27 \in (3)$ ✓

$\supseteq$ $3 = 27 - 4 \cdot 6 \in (6, 15, 27)$.

- des Ideals $(6, 15, 27)$ in $\mathbb{Z}$

- des Ideals $(X^p - 1,\ p \text{ Primzahl}) = (X^2 - 1, X^3 - 1, X^5 - 1, \dots)$ in $\mathbb{C}[X]$

$\| $

$(X - 1)$

Der Euklidische Algorithmus
Vorlesungswoche 2

Ulrich Görtz

Lineare Algebra 2, SS 21

UNIVERSITÄT
DUISBURG
ESSEN

Der größte gemeinsame Teiler

Sei R ein Integritätsbereich.

Def. Seien $a, b \in R$

(1) Ein Element $d \in R$ heißt *größter gemeinsamer Teiler* von a, b, falls $d \mid a$ und $d \mid b$, und für alle $d' \in R$ mit $d' \mid a$ und $d' \mid b$ gilt: $d' \mid d$. $\quad ggT(a,b)$

(2) Ein Element $m \in R$ heißt *kleinstes gemeinsames Vielfaches* von a und b, falls $a \mid m$ und $b \mid m$, und für alle $m' \in R$ mit $a \mid m'$ und $b \mid m'$ gilt $m \mid m'$. $\quad kgV(a,b)$

Bem.

- $d \mid a \iff (a) \subseteq (d) \Rightarrow d' \in R$ ist gem. Teiler von a, b $\iff (a,b) \subseteq (d')$
- Folgerung: wenn (a,b) Hauptideal, etwa $(a,b) = (d) \Rightarrow d$ ist ggT von a, b.

Der euklidische Algorithmus

Seien R ein euklidischer Ring mit Gradabb. δ.

Seien $a, b \in R \setminus \{0\}$.

Wir setzen $a_0 := a$, $a_1 := b$ und definieren für $i > 1$ den Elem. $a_i \in R$ durch $a_{i-2} = q_{i-1} \cdot a_{i-1} + a_i$ $\left(\underbrace{a_i = 0 \text{ oder } \delta(a_i) < \delta(a_{i-1})}_{\circledast}\right)$

Der Algorithmus endet, wenn $a_{k+1} = 0$ (das ist wegen $\circledast$ weil endlich viele Schritte der Fall).

Dann ist a_k ein ggT von a und b:

Es genügt dafür zu sehen, dass $(a, b) = (a_k)$. Wegen der Gleichung, die a_i definiert, gilt immer $(a_{i-1}, a_{i-2}) = (a_{i-1}, a_i)$, d.h.

$$(a,b) = (a_0, a_1) = (a_1, a_2) = \cdots = (a_{k-1}, a_k) = (a_k, a_{k+1}) = (a_k)$$

($a_{k+1} = 0$)

Indem man die obigen Gleichungen "rückwärts einsetzt":

$$a_k = a_{k-2} - q_{k-1}\, a_{k-1} = a_{k-2} - q_{k-1}\left(a_{k-3} - q_{k-2}\, a_{k-2}\right) = \dots$$

dann erhält man eine Darstellung $a_k = x \cdot a + y \cdot b, \quad x, y \in \mathbb{R}$.

Quiz

Bestimmen Sie mit dem euklidischen Algorithmus den größten gemeinsamen Teiler von 12345 und 54321 in $\mathbb{Z}$.

Quiz

Bestimmen Sie mit dem euklidischen Algorithmus den größten gemeinsamen Teiler von 12345 und 54321 in $\mathbb{Z}$.

Eukl. Algorithmus:

$$54321 = 4 \cdot 12345 + 4941$$
$$12345 = 2 \cdot 4941 + 2463$$
$$4941 = 2 \cdot 2463 + 15$$
$$2463 = 164 \cdot 15 + 3$$
$$15 = 5 \cdot 3 + 0$$

$\rightsquigarrow$ 3 ist ggT von 54321 und 12345.

Quiz

Bestimmen Sie mit dem euklidischen Algorithmus den größten gemeinsamen Teiler von 12345 und 54321 in $\mathbb{Z}$.

Eukl. Algorithmus:

$$54321 = 4 \cdot 12345 + 4941$$
$$12345 = 2 \cdot 4941 + 2463$$
$$4941 = 2 \cdot 2463 + 15$$
$$2463 = 164 \cdot 15 + 3$$
$$15 = 5 \cdot 3$$

$\rightsquigarrow$ 3 ist ggT von 54321 und 12345.

$$3 = 2463 - 164 \cdot 15 = 2463 - 164 \cdot (4941 - 2 \cdot 2463)$$
$$= \dots = 3617 \cdot 12345 - 822 \cdot 54321.$$

Quiz

Seien $f = X^3 - 2X^2 - 9$ und $g = X^2 - 5X + 6$ (in $\mathbb{Q}[X]$).

Bestimmen Sie mit dem euklidischen Algorithmus Polynome $p, q \in \mathbb{Q}[X]$, so dass $pf + qg = 1$ gilt.

Quiz

Seien $f = X^3 - 2X^2 - 9$ und $g = X^2 - 5X + 6$ (in $\mathbb{Q}[X]$).

Bestimmen Sie mit dem euklidischen Algorithmus Polynome $p, q \in \mathbb{Q}[X]$, so dass $pf + qg = 1$ gilt.

Eukl. Algorithmus:

$$X^3 - 2X^2 - 9 = (X+3)(X^2 - 5X + 6) + (9X - 27)$$

$$X^2 - 5X + 6 = \tfrac{1}{9}(X-2) \cdot (9X - 27)$$

$\rightsquigarrow$ $9X - 27$ ist ggT von f, g, also auch: $X - 3$ ist ggT von f, g

$$X - 3 = \tfrac{1}{9}(X^3 - 2X^2 - 9) - \tfrac{1}{9}(X+3)(X^2 - 5X + 6) = \underbrace{\tfrac{1}{9}}_{p} \cdot f \underbrace{- \tfrac{1}{9}(X+3)}_{q} \cdot g.$$

Irreduzible Elemente und Primelemente
Vorlesungswoche 2

Ulrich Görtz

Lineare Algebra 2, SS 21

UNIVERSITÄT
DUISBURG
ESSEN

Primzahlen

in allg. Ringen R werden durch $p \in R \setminus (R^\times \cup \{0\})$

Def. Eine ganze Zahl $p > 1$ heißt Primzahl, wenn gilt: Sind $a, b \in \mathbb{Z}$ mit $p = ab$, dann ist $a \in \mathbb{Z}^\times$ oder $b \in \mathbb{Z}^\times$.
$\mathbb{Z}^\times = \{1, -1\}$

Primeigenschaft Eine ganze Zahl $p > 1$ hat die Primeigenschaft, wenn gilt: Sind $a, b \in \mathbb{Z}$ mit $p \mid ab$, dann $p \mid a$ oder $p \mid b$.

- Leicht: Hat $p > 1$ die Primeigenschaft, dann ist p eine Primzahl
- Jede Primzahl $\in \mathbb{Z}$ hat die Primeigenschaft.

Irreduzible Elemente, Primelemente

Def. Sei R ein Integritätsring.

(1) Ein Element $p \in R \setminus (R^\times \cup \{0\})$ heißt *irreduzibel*, wenn gilt:
Sind $a, b \in R$ mit $p = ab$, dann ist $a \in R^\times$ oder $b \in R^\times$.

(2) Ein Element $p \in R \setminus (R^\times \cup \{0\})$ heißt *prim*, wenn gilt:
Sind $a, b \in R$ mit $p \mid ab$, dann gilt $p \mid a$ oder $p \mid b$.

Bem. Sei $p \in R \setminus (R^\times \cup \{0\})$ mit $p = ab$. Dann $a \in R^\times \iff p$ und b assoziiert
("$\Rightarrow$" klar. "$\Leftarrow$" Sei etwa $p = ub$, $u \in R^\times$.
Dann $ub = p = ab$, also (denn $b \neq 0$, R Integritätsring)
$u = a$.)

Quiz

Die Teilmenge $R = \{\sum_{i=0}^{n} a_i X^i;\ n \in \mathbb{N}, a_i \in \mathbb{Q}, a_1 = 0\} \subseteq \mathbb{Q}[X]$ ist ein Unterring.

- Ist X^2 ein irreduzibles Element von R?
- Ist X^2 ein Primelement von R?

Quiz

Die Teilmenge $R = \{\sum_{i=0}^{n} a_i X^i;\ n \in \mathbb{N}, a_i \in \mathbb{Q}, a_1 = 0\} \subseteq \mathbb{Q}[X]$ ist ein Unterring.

Ist X^2 ein irreduzibles Element von R? Ja, denn aus $X^2 = f \cdot g$ folgt $\deg(f) + \deg(g) = 2$, und in R liegen keine Polynome mit Grad 1, und alle Polynome vom Grad 0 sind Einheiten

Ist X^2 ein Primelement von R?

Nein, denn

$X^2 \mid X^3 \cdot X^3$,

aber $X^2 \nmid X^3$.

$X^6 = X^4 \cdot X^2$

$\in R$

Prim impliziert irreduzibel

$p \mid ab \Rightarrow p \mid a$ oder $p \mid b$

Satz Sei R ein Integritätsbereich und $p \in R \setminus (R^\times \cup \{0\})$ prim.
Dann ist p irreduzibel.

Beweis Seien $a, b \in R$ mit $p = ab$. Zz: p ist assoziiert zu a oder zu b.

Aus $p = ab$ folgt $p \mid ab$, also $p \mid a$ oder $p \mid b$, weil p prim ist.

Sei OE $p \mid a$.

Andererseits folgt aus $p = ab$, dass $a \mid p$ $\Big\}$ $\Rightarrow$ a, p assoziiert zueinander.

Primelemente in Hauptidealringen

Satz Sei R ein Hauptidealring, $p \in R \setminus (R^\times \cup \{0\})$ irreduzibel.
Dann ist p prim.

Beweis Seien $a, b \in R$ mit $p \mid ab$. Gelte $p \nmid a$. zz: $p \mid b$.

Dass $p \nmid a$ ist dem äquivalent, dass $(a) \not\subseteq (p)$.

Dann gilt $(p) \subsetneq (p, a)$. Weil R HIR, ex. $d \in R$ mit $(p, a) = (d)$.

Also gilt $(p) \subsetneq (d)$. Weil $p \in (d)$, etwa $p = xd$, $x \in R$.

$\Longrightarrow$ p assoz zu d oder $d \in R^\times$

p irred.

$\to (p) = (d)$ ↯

$\Rightarrow (p, a) = (d) = R \ni 1$

↳ Das kann man, denn es ex. mit $xp + ya = 1$

(Denn $(p, a) = \{xp + ya ; x, y \in R\}$)

Also gilt $p \mid xp = 1 - ya$, folglich $p \mid b - yab$

Weil $p \mid ab$, folgt $p \mid b$.