Wiederholungen

- $0 \neq f \in K[X]$

  f zerfällt in Linearfaktoren $:\Leftrightarrow$

  es ex. $c, a_1, \dots, a_\ell \in K$, $m_1, \dots, m_\ell \in \mathbb{N}$: $f = c(X-a_1)^{m_1} \cdots (X-a_\ell)^{m_\ell}$

- K algebraisch abgeschlossen $:\Leftrightarrow$ Jeder $0 \neq f \in K[X]$ zerfällt in Linearfaktoren

- $\mathbb{C}$ ist algebraisch abgeschlossen (ohne Beweis)

- $a, b \in \mathbb{Z}$, $a, b \neq 0$

  $V := \{ v \in \mathbb{N} \mid a \text{ teilt } v \text{ u. } b \text{ teilt } v \}$

  besitzt Minimum bzgl. „|", $kgV(a,b)$

  $kgV(a,0) := 0$.

  $r := kgV(a,b)$. Dann: - $a \mid r$ und $b \mid r$

  - Ist $r' \in \mathbb{Z}$ mit $a \mid r'$ und $b \mid r'$, dann ist $r \mid r'$

  Analog für $K[X]$.

- $ggT(a,b)\, k(a,b) = |ab|$ ~~falls $a, b \neq 0$~~

- $R = \mathbb{Z}$, oder $R = K[X]$
  - R ist Hauptidealring, d.h. R ist Integritätsbereich und jedes Ideal ist Hauptideal
- $a, b \in \mathbb{Z}^*$, $b \neq 0$

  $D := \{d \in \mathbb{N} \mid d \text{ teilt } a \text{ u. } d \text{ teilt } b\}$

  D besitzt Maximum bzgl „$|$“ : $ggT(a,b)$

  $ggT(a,0) := |a|$.

  $ggT(a,b) = \lambda a + \mu b$, für geeign. $\lambda, \mu \in \mathbb{Z}$

  $d := ggT(a,b)$; Dann: - $d \mid a$ und $d \mid b$
  - Ist $d' \in \mathbb{Z}$ mit $d' \mid a$ und $d' \mid b$, dann ist $d' \mid d$

Analog für $K[X]$.

Erweiterter Euklidischer Algorithmus:

gegeben $a, b \in R, b \neq 0$

liefert $ggT(a,b), \lambda, \mu \in R$ mit $ggT(a,b) = \lambda a + \mu b$

EUKLID(a,b)

1. Bestimme $q, r \in R$ mit $a = qb + r$ mit $v(r) < v(b)$
2. If $r = 0$ $\quad\quad \lambda \quad \mu$
3. return $(|b|, 0, |b|/b)$
4. else $(d, \lambda, \mu) \leftarrow$ EUKLID(b, r)
5. return $(d, \mu, \lambda - q\mu)$.

Beweis der Korrektheit: 1. Fall: $r=0$, $|b| = ggT(qb, b)$, $|b| = 0 \cdot a + \frac{|b|}{b} \cdot b$

2. Fall: $r \neq 0$ $\quad d = ggT(b,r) = ggT(a,b)$

λ, μ so, dass $\quad d = \lambda b + \mu r = \lambda b + \mu(a - qb)$

$= \mu a + (\lambda - q\mu) b.$ ▨

Kongruenzen und Restklassenringe

Setup

- $R = \mathbb{Z}$ oder $R = K[X]$ für einen Körper K
- $m \in R \setminus \{0\}$, [illegible] $m \in \mathbb{N}$, falls $R = \mathbb{Z}$

(m steht für *modulus*, lat. Maß.)

Kongruenzen

Definition

$a, b \in R$

$a \equiv_m b :\Leftrightarrow m \mid a - b$

Wir lesen $a \equiv_m b$ als „a kongruent b modulo m“.

Beispiele

- in $\mathbb{Z}$:
  - $7 \equiv_7 0$
  - $1 \equiv_7 8$
  - $1 \equiv_7 -6$
  - $3 \equiv_7 10$
  - $2 \equiv_7 9$
  - $2 \equiv_7 16$
  - $2 \equiv_7 -5$
  - $16 \equiv_7 -5$
- in $\mathbb{Q}[X]$:
  - $X^2 - 1 \equiv_{X^2-1} 0$
  - $X^2 \equiv_{X^2-1} 1$
  - $X^4 - X^2 + 1 \equiv_{X^2-1} 1$

Kongruenzen (Forts.)

Proposition

$\equiv_m$ ist Äquivalenzrelation auf R.

$R / \equiv_m$

Notation

- Äquivalenzklasse von $a \in R$ wird mit $\overline{a}$ bezeichnet.
- $R/(m) := \{\overline{a} \mid a \in R\}$ Menge der Äquivalenzklassen.
- Für $R = \mathbb{Z}$ schreiben wir auch $\mathbb{Z}_m := \mathbb{Z}/(m)$.

Beweis der Proposition:

(R) $a \equiv_m a$ ✓ da $m \mid a-a$

(S) $a \equiv_m b \Rightarrow b \equiv_m a$ ✓ $m \mid a-b \Rightarrow m \mid \underbrace{(-1)(a-b)}_{b-a}$

(T) $a \equiv_m b,\ b \equiv_m c \Rightarrow a \equiv_m c$ ✓

$m \mid a-b$ u. $m \mid b-c \Rightarrow m \mid \underbrace{(a-b)+(b-c)}_{a-c}$

Kongruenzen (Forts.)

Beispiele

- in $\mathbb{Z}_7$:
  - $\overline{7} = \overline{0}$
  - $\overline{1} = \overline{8} = \overline{-6}$
  - $\overline{3} = \overline{10}$
  - $\overline{2} = \overline{9} = \overline{16} = \overline{-5}$
- in $\mathbb{Q}[X]/(X^2 - 1)$:
  - $\overline{X^2 - 1} = \overline{0}$
  - $\overline{X^2} = \overline{X^4 - X^2 + 1} = \overline{1}$

Kongruenzen und Division mit Rest

Definition

Es sei $a \in R$. Dividiere a durch m mit Rest:

$$a = qm + r$$

mit

$$\begin{cases} 0 \leq r < m, & \text{im Fall } R = \mathbb{Z}, \\ \deg r < \deg m, & \text{im Fall } R = K[X]. \end{cases}$$

Wir setzen

$$a \bmod m := r.$$

Beispiele

- $101 \bmod 7 = 3$;
- $1001 \bmod 13 = 0$;
- $X^3 - 2X^2 + 5 \bmod (X^2 + X + 1) = 2X + 8$.

Kongruenzen und Division mit Rest (Forts.)

Proposition

(a) ▸ Für alle $a \in R$ gilt: $a \equiv_m a \bmod m$.

(b) ▸ Es seien $a, b \in R$.

Dann sind äquivalent:

- $a \equiv_m b$
- $a \bmod m = b \bmod m$

Beweis der Proposition:

(a) $a = qm + r = qm + (a \bmod m)$

$\Rightarrow m \mid qm$, $qm = a - (a \bmod m)$ ✓ ∎

(b) $a \bmod m = b \bmod m \iff$

es ex. $q_1, q_2, r \in \mathbb{R}$: $a = q_1 m + r$, $b = q_2 m + r$ $\iff$

es ex. $q_1, q_2, r \in \mathbb{R}$: $a - b = (q_1 - q_2) m$ $\iff$

$m \mid a - b$ $\iff$

$a \equiv_m b$. ∎

Kongruenzen und Division mit Rest (Forts.)

Bemerkung

Für $a \in R$ ist

$$\bar{a} = a + Rm$$

mit $a + Rm = \{a + xm \mid x \in R\}$.

Ist $r := a \bmod m$, dann ist $\bar{a} = \bar{r}$, d.h.

$\bar{a} = \{ r + xm \mid x \in R \}$ Restklasse

$m = 2$, $R = \mathbb{Z}$: $\bar{0} = 2\mathbb{Z}$ geraden Zahlen

$\bar{1} = 1 + 2\mathbb{Z}$ ungeraden Zahlen

$m = 3$, $R = \mathbb{Z}$: $\bar{0} = 3\mathbb{Z}$, $\bar{1} = 1 + 3\mathbb{Z}$, $\bar{2} = 2 + 3\mathbb{Z}$

Beweis der Bemerkung: Sei $a \in R$.

$b \in \bar{a} \iff a \equiv_m b$

$\iff m \mid a-b$

$\iff$ es ex. $z \in R$ mit $a-b = zm$

$\iff$ es ex. $z \in R$ mit $b = a + (-z)m$. ∎

Kongruenzen und Division mit Rest (Forts.)

Definition

Es sei $n \in \mathbb{N}_0$. Wir setzen

$$\begin{aligned} K[X]_{<n} &:= \{f \in K[X] \mid \deg f < n\} \\ &= \{\sum_{i=0}^{n-1} a_i X^i \mid a_0, a_1, \ldots, a_{n-1} \in K\}. \end{aligned}$$

Beipiele

- $K[X]_{<0} = \{0\}$.
- $K[X]_{<1} = \{f \in K[X] \mid f \text{ ist konstant}\} = K$.
- $K[X]_{<2} = \{aX + b \mid a, b \in K\}$: Menge der linearen Polynome.

Kongruenzen und Division mit Rest (Forts.)

Korollar

- Es sei $n \in \mathbb{N}$.

  $\{0, 1, \ldots, n-1\}$ ist Repräsentantensystem von $\mathbb{Z}/(n)$; insbesondere:

$$\mathbb{Z}_n = \mathbb{Z}/(n) = \{\overline{r} \mid r \in \{0, 1, \ldots, n-1\}\}.$$

- Es sei $g \in K[X] \setminus \{0\}, n := \deg g$.

  $K[X]_{<n}$ ist Repräsentantensystem von $K[X]/(g)$; insbesondere:

$$K[X]/(g) = \{\overline{r} \mid r \in K[X]_{<n}\}.$$

Kongruenzen und Division mit Rest (Forts.)

Beispiel

- $\mathbb{Z}/(7) = \quad \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$
- $\mathbb{Q}[X]/(X^2-1) = \quad \{\bar{f} \mid f \in \mathbb{Q}[X]_{<2}\}$

$$= \{\overline{aX+b} \mid a,b \in \mathbb{Q}\}.$$

Restklassenringe

Proposition

Es seien $a, a', b, b' \in R$ mit $a \equiv_m a'$, $b \equiv_m b'$. Dann gilt:

(a) ▶ $a + b \equiv_m a' + b'$;

(b) ▶ $ab \equiv_m a'b'$.

Beweis: (a) $m \mid a - a'$, $m \mid b - b' \Rightarrow m \mid \underbrace{(a - a') + (b - b')}_{(a+b) - (a'+b')}$

(b) $m \mid a - a'$, $m \mid b - b'$

$\Rightarrow m \mid \underbrace{(a - a')b + (b - b')a'}_{ab - a'b'}$ ▨

Restklassenringe (Forts.)

Beispiel

In $\mathbb{Q}[X]$:

$f := X^5 - 3X^4 + 2X^3 - X^2 + 2, h := X^4 - X^3 + 2.$

$$\begin{aligned} f &\equiv_{X^2-1} 3X - 2 \\ h &\equiv_{X^2-1} -X + 3 \end{aligned}$$

$$\begin{aligned} f + h &\equiv_{X^2-1} 2X + 1 \\ f \cdot h &\equiv_{X^2-1} -3X^2 + 11X - 6 \end{aligned}$$

Wegen $-3X^2 + 11X - 6 \bmod X^2 - 1 = 11X - 9$ gilt auch

$$f \cdot h \equiv_{X^2-1} 11X - 9.$$

Restklassenringe (Forts.)

Proposition

$R/(m)$ wird kommutativer Ring mit:

- Addition: $\bar{a} + \bar{b} := \overline{a+b}$
- Null: $0 = \bar{0}$
- Negative: $-\bar{a} = \overline{-a}$
- Multiplikation: $\bar{f} \cdot \bar{g} := \overline{f \cdot g}$
- Eins: $1 = \bar{1}$

AG, KG, DG folgen aus denen von R.

Restklassenringe (Forts.)

Beispiele

$\overline{6}^{100\,000} = \overline{(-1)}^{100\,000} = \overline{1}$.

- In $\mathbb{Z}/(7)$:
  - $\overline{5}+\overline{4} = \overline{9} = \overline{2}$
  - $\overline{3}\cdot\overline{4} = \overline{3\cdot 4} = \overline{12} = \overline{5}$
  - $\overline{13}\cdot\overline{13} = \overline{6}\cdot\overline{6} = \overline{(-1)}\cdot\overline{(-1)} = \overline{(-1)\cdot(-1)} = \overline{1}$.

- In $\mathbb{Q}[X]/(X^2-1)$:
  - $\overline{X^5-X^3-3}\cdot\overline{X^4-X^2+2} = \overline{-3}\cdot\overline{2} = \overline{-6}$
  - $\overline{X-1}\cdot\overline{X+1} = \overline{0}$

Quersummenregl: $n \in \mathbb{Z}$ ist durch 3 teilbar $\iff$
Quersumme von n ist durch 3 teilbar

Beweis: $n = \sum_{i=0}^{k} z_i \cdot 10^i \qquad z_i \in \{0, 1, \dots, 9\}.$

Rechne modulo 3. $\bar{1}\bar{0} = \bar{1}$

$$3 \mid n \iff \bar{n} = \bar{0}$$

$$\iff \bar{0} = \sum_{i=0}^{k} \bar{z}_i \cdot \bar{1} = \sum_{i=0}^{k} \bar{z}_i = \overline{\sum_{i=0}^{k} z_i}$$

Restklassenringe (Forts.)

Bemerkung (Rechnen in $\mathbb{Z}_n$)

Es seien $i, j \in \mathbb{Z}$ mit $0 \leq i, j < n$.

- Zur Addition von $\bar{i}$ und $\bar{j}$, addiere i und j in $\mathbb{Z}$ und dividiere das Ergebnis mit Rest durch n:

$$\bar{i} + \bar{j} = \overline{(i + j) \bmod n}.$$

- Zur Multiplikation von $\bar{i}$ und $\bar{j}$, multipliziere i und j in $\mathbb{Z}$ und dividiere das Ergebnis mit Rest durch n:

$$\bar{i} \cdot \bar{j} = \overline{(i \cdot j) \bmod n}.$$

Analoge Regeln gelten für das Rechnen im Restklassenring $K[X]/(g)$ für ein $g \in K[X] \setminus \{0\}$.

Restklassenringe (Forts.)

Beispiel

Addition und Multiplikation von $\mathbb{Z}/(4) = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Lineare Kongruenzgleichungen in einer Unbekannten

Lösbarkeitskriterium für lineare Kongruenzgleichungen

Es seien $a, b \in R$. Dann gilt:

Es gibt $x \in R$ mit $xa \equiv_m b \Leftrightarrow \mathrm{ggT}(a, m) \mid b$.

Korollar

Es sei $a \in R$. Dann gilt: $\overline{a} \in (R/(m))^\times \Leftrightarrow \mathrm{ggT}(a, m) = 1$.

Folgt aus Kriterium für $b = 1$.

Beweis des Lösbarkeitskriteriums:

„$\Rightarrow$" $\quad m \mid xa - b$

$$\Rightarrow \left.\begin{array}{l} ggT(a,m) \mid xa - b \\ ggT(a,m) \mid a \end{array}\right\} \Rightarrow ggT(a,m) \mid b$$

„$\Leftarrow$" Sei $q \in \mathbb{R}$ mit $q \cdot ggT(a,m) = b$

Seien $\lambda, \mu \in \mathbb{R}$ mit $ggT(a,m) = \lambda a + \mu m$

$\Rightarrow (q\lambda)a + (q\mu)m = b$

$\Rightarrow m \mid (q\lambda)a - b$

$\Rightarrow (q\lambda)a \equiv_m b$. ∎

Einheiten (Forts.)

Korollar

Es sei $a \in R$. Dann gilt: $\overline{a} \in (R/(m))^\times \Leftrightarrow \mathrm{ggT}(a, m) = 1$.

Bemerkung

Es sei $a \in R$ mit $\mathrm{ggT}(a, m) = 1$.

Frage: Wie findet man $\overline{a}^{-1} \in R/(m)$?

Antwort: Bestimme $x, y \in R$ mit $xa + ym = 1$.

Dann ist $\overline{a}^{-1} = \overline{x}$. Denn $m \mid xa - 1$, d.h. $xa \equiv_m 1$,
d.h. $\overline{x} \cdot \overline{a} = \overline{1}$

Einheiten (Forts.)

Beispiele

- $\overline{17} \in (\mathbb{Z}/(30))^\times$ mit

$$\overline{17}^{-1} = \overline{23} \qquad 17 \cdot 23 = 391, \; 391 \equiv_{30} 1$$

- $\overline{X+2} \in (\mathbb{Q}[X]/(X^2-1))^\times$ mit

$$(\overline{X+2})^{-1} = \overline{-X/3+2/3}$$

$$\tfrac{1}{3}(X+2)(-X+2) = \tfrac{1}{3}(-X^2+4)$$

$$= \tfrac{1}{3}(-X^2+1) + 1 .$$

- $(\mathbb{Z}_8)^\times =$

$\{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$.

Einheiten (Forts.)

Definition

- Ein Element $p \in \mathbb{N}$ heißt *Primzahl*, wenn $p > 1$ ist und 1 und p die einzigen Teiler von p in $\mathbb{N}$ sind.

- Ein Element $g \in K[X]$ heißt *irreduzibel*, wenn $g \neq 0$ ist, $\deg g \geq 1$ ist und es gilt: die einzigen Teiler von g sind Einheiten oder assoziiert zu g.

  Mit anderen Worten: Ist $g = fh$ mit $f, h \in K[X]$, dann ist $f \in K^\times$ oder $h \in K^\times$.

Einheiten (Forts.)

Satz

Es sei $m \in R, m \neq 0$. Dann sind äquivalent:

- $R/(m)$ ist Körper
- $\begin{cases} m \text{ ist Primzahl} & (\text{im Fall } R = \mathbb{Z}) \\ m \text{ ist irreduzibel} & (\text{im Fall } R = K[X]) \end{cases}$

Beweis: Für $a \in R$ gilt:

$\bar{a} \neq \bar{0} \iff m \nmid a$

$\iff ggT(a, m) = 1$

$\leftarrow$ da m Primzahl (bzw. irreduzibel).