

Korrektur von Vorlesung 7.

Def: Ein Element $p \neq 0$, p keine Einheit, heisst prim falls

$$p \mid ab \Rightarrow p \mid a \text{ oder } p \mid b \quad \forall a, b \in R$$

(nicht $p = ab \Rightarrow \dots$)

Lemma 3.1: Sei $(R, +, \cdot)$ ein Ring mit Eins und ohne Nullteiler

und $a \in R$

a ist prim $\Rightarrow a$ ist irreduzibel

aber die Rückrichtung gilt nicht unbedingt.

Beispiele

	1. Kommutativ + Assoziativ	2. Assoziativ	3. + Identität	4. + Inverse	5. Kommutativ	6. Assoziativ	7. Distributiv	8. Identität	weitere Kommentare
$R_1: \mathbb{Z}^2$ $(a,b) + (c,d) := (a+c, b+d)$ $(a,b) \cdot (c,d) := (ac, bd)$	✓	✓	✓ $O_{R_1} = (0,0)$	✓ $-(a,b) = (-a,-b)$	✓	✓	✓	✓ $1_{R_1} = (1,1)$	$(0,1) \cdot (1,0) = O_{R_1}$ hat Nullteiler
$R_2: \mathbb{R}^{\mathbb{R}} = \{f: \mathbb{R} \rightarrow \mathbb{R}\}$ $(f+g)(x) := f(x) + g(x)$ $(f \cdot g)(x) := f(x) \cdot g(x)$	✓	✓	✓ $O_{R_2} = f: \mathbb{R} \rightarrow \mathbb{R}, x \mapsto 0$	✓ $f: \mathbb{R} \rightarrow \mathbb{R}, x \mapsto f(x)$	✓	✓	✓	✓ $1_{R_2} = f: \mathbb{R} \rightarrow \mathbb{R}, x \mapsto 1$	hat Nullteiler
$R_3: \mathbb{R}^{\mathbb{R}}$ $(f+g)(x) := f(x) + g(x)$ $(f \cdot g)(x) := f(g(x))$	✓	✓	✓	✓	✗ $f(x) = e^x$ $g(x) = x^2$ $e^{(x^2)} \neq (e^x)^2$	✓	! $(f \cdot g) \cdot h \neq f \cdot (g \cdot h)$	✓ $1_{R_3} = f: \mathbb{R} \rightarrow \mathbb{R}, x \mapsto x$	R_3 nicht ein Ring auch kein nicht-kommutativer (wäre aber ein nicht-kommut. Ring wenn wir auf lineare Funktionen einschränken würden)
$R_4: R$ $x +_{R_4} y := (x^3 + y^3)^{1/3}$ $x \cdot_{R_4} y := x \cdot y$	✓	✓ $(x^3 + (y^3 + z^3))^{1/3} = (x^3 + y^3 + z^3)^{1/3}$ $= (x^3 + y^3 + z^3)^{1/3}$	✓ $O_{R_4} = 0$	✓ $_{R_4} x = -x$	✓	✓	✓ $x \cdot (y^3 + z^3)^{1/3} = (x^3 y^3 + x^3 z^3)^{1/3} = x \cdot y + x \cdot z$	✓ $1_{R_4} = 1$	

$R_5: \{0, \text{Romney, Obama}\}$

+	0	Ro	Ob
0	0	Ro	Ob
Ro	0	Ro	Ob
Ob	0	Ob	Ro

esl ein Ring mit Eins

$(R_5, 1_{R_5} = \text{Romney})$

Dieser Ring ist isomorph zu $\mathbb{Z}/3\mathbb{Z}$

Def: Ein Körper ist ein Ring mit Eins und mit der zusätzlichen Eigenschaft

$$9. \forall a \in R \setminus \{0\} \exists b \in R \text{ sodass } a \cdot b = b \cdot a = 1$$

Multiplikative Inverse

(dieses Element b bezeichnen wir mit a^{-1})

z.B. $\mathbb{R}_4, \mathbb{R}_5, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ sind Körper

Ein weiteres wichtiges Beispiel:

Def: Sei R ein Ring. Der Polynomring über R ist

$$\begin{aligned} R[X] &:= \{ r_n X^n + r_{n-1} X^{n-1} + \dots + r_1 X + r_0 : n \in \mathbb{N}, r_i \in R \} \\ &= \left\{ \sum_{i=0}^n r_i X^i : n \in \mathbb{N}, r_i \in R \right\} \end{aligned}$$

$$\text{mit } \left(\sum_{i=0}^n r_i X^i \right) + \left(\sum_{j=0}^m s_j X^j \right) := \sum_{k=0}^{\max(n,m)} (r_k + s_k) X^k$$

(wobei $r_k = 0$ für $n < k \leq m$
 $s_k = 0$ für $m < k \leq n$)

$$\text{und } \left(\sum_{i=0}^n r_i X^i \right) \cdot \left(\sum_{j=0}^m s_j X^j \right) := \sum_{k=0}^{m+n} \left(\sum_{\substack{i+j=k \\ 0 \leq i \leq n \\ 0 \leq j \leq m}} r_i s_j \right) X^k$$

(übliche Addition und Multiplikationsregeln)

Bemerkung: $R[X]$ ist ein Ring

$$R[X] \text{ hat Eins} \Leftrightarrow R \text{ hat Eins}$$

Ein Sonderfall: Sei $n \in \mathbb{Z}$ und $m \notin \mathbb{Z}$ aber $m^2 = n$

Dann sind $1, m^2, m^4, m^6, \dots \in \mathbb{Z}$

und $m, m^3, m^5, m^7, \dots \in m\mathbb{Z}$

also ist $\mathbb{Z}[m] = \{a + bm : a, b \in \mathbb{Z}\}$

z.B. $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\} \subset \mathbb{R}$

$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\} \subset \mathbb{C}$ (die Gaußschen Zahlen)

Ähnlich ist $\mathbb{Q}[m]$ für $m^2 \in \mathbb{Q}$

siehe später: Quadratische Zahlkörper

Wir betrachten jetzt $\mathbb{C}[X]$, die komplexen Polynome

Def: Sei $f(x) = \sum_{i=0}^n a_i X^i$, wobei $a_i \in \mathbb{C}$ und $a_n \neq 0$

Der Grad von f ist $\text{Grad}(f) := n$

Ein normiertes Polynom ist ein Polynom der Form

$X^n + a_{n-1}X^{n-1} + \dots + a_1X + a_0$ (Grad n und $a_n = 1$)

Sei $I \subseteq \mathbb{C}[X]$ die Menge aller irreduziblen normierten Polynome

Nach dem Fundamentalsatz der Algebra sind das die normierten Polynome von Grad 1, d.h. die linearen normierten Polynome.

(Die Polynome von Grad 0, d.h. die konstanten Polynome ungleich 0, sind die Einheiten von $\mathbb{C}[X]$.)

Beimerkung: Zwei Polynome $f, g \in \mathbb{C}[X]$ heissen teilerfremd
wenn $\forall h \in \mathbb{C}[X]$ gilt
 $h|f$ und $h|g \Rightarrow \text{Grad}(h) = 0$

Der ABC-Satz für Polynome

Satz 3.2 (Mason, Stothers):

Seien $A, B, C \in \mathbb{C}[X]$ teilerfremd mit $A + B = C$
und $\text{Grad}(C) = \max(\text{Grad}(A), \text{Grad}(B)) \geq 1$

Dann gilt $\text{Grad}(C) < \text{Grad}\left(\prod_{\substack{P \in I \\ P|ABC}} P\right)$

Vorbemerkungen zum Beweis

Def: Seien $f, g \in \mathbb{C}[X]$. Der größte gemeinsame Teiler von f und g
ist das (eindeutige) normierte Polynom h des größten Grades
sodass $h|f$ und $h|g$

Bezeichnet $\text{ggT}(f, g)$

$$N_0(f) := \text{Grad}\left(\prod_{\substack{P \in I \\ P|f}} P\right)$$

= Anzahl der verschiedenen Nullstellen von f .

Beispiel: $f(x) = x^5 (x-2)^3 (2x+8)^2 (x+4)^3$

$$g(x) = (x+\sqrt{2}i)^2 (x-2)^2 (x+4)^4$$

$$\text{Grad}(f) = 5 + 3 + 2 + 3 = 13$$

$$\text{Grad}(g) = 8$$

$$\text{ggT}(f, g) = (x-2)^2 (x+4)^4$$

$$N_0(f) = \text{Grad}(x(x-2)(x+4)) = 3$$

Lemma 3.3: Ein Polynom $f \in \mathbb{C}[X]$ hat eine Nullstelle α mit Vielfachheit $k \geq 1 \iff \alpha$ ist eine Nullstelle von f' mit Vielfachheit $k-1$.

Lemma 3.4: Sei $f \in \mathbb{C}[X]$. Dann ist

$$\text{Grad}(\text{ggT}(f, f')) = \text{Grad}(f) - N_0(f)$$

Beweis: Nächstes Mal.