

Ringe

Definition 109

Ein Ring R ist eine Menge R zusammen mit zwei Verknüpfungen $+ : R \times R \rightarrow R$, $\cdot : R \times R \rightarrow R$, so dass

(1) $(R, +)$ ist eine abelsche Gruppe

$$(2) \quad \forall r_1, r_2, r_3 \in R: (r_1 \cdot r_2) \cdot r_3 = r_1 \cdot (r_2 \cdot r_3) \quad (\text{Assoz.-gesetz})$$

$$(r_1 + r_2) \cdot r_3 = r_1 \cdot r_3 + r_2 \cdot r_3 \quad (\text{Distributiv-})$$

$$r_1 \cdot (r_2 + r_3) = r_1 \cdot r_2 + r_1 \cdot r_3 \quad (\text{gesetz})$$

$$(3) \quad \exists 1 \in R: \forall r \in R: 1 \cdot r = r \quad (\text{neutr. El. bzgl. \(\cdot\)})$$

Wir bezeichnen das neutr. Element bzgl. $+$ mit 0 .

Ein Ring heißt Kommutativ, falls gilt: $\forall r_1, r_2 \in R: r_1 \cdot r_2 = r_2 \cdot r_1$

Definition 110

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

$$R^* := \{r \in R \mid \exists s \in R \text{ mit } r \cdot s = 1\}$$

die Einheiten in R .

Bemerkung: (a) (R^*, \cdot) ist eine Gruppe.

(b) R ist ein Körper genau dann, wenn $R^* = R \setminus \{0\}$.

Beispiele von Ringen: $(\mathbb{Z}, +, \cdot)$ ist ein kommutativer Ring

$(\mathbb{Q}[x], +, \cdot)$ ist ein kommutativer Ring.

$(\mathbb{R}^{n \times n}, +, \cdot)$ ist ein nicht-kommutativer Ring.
 $((\mathbb{R}^{n \times n})^\times = GL(n, \mathbb{R}) := \{ A \in \mathbb{R}^{n \times n} \mid \det(A) \neq 0 \})$

Definition 111

Sei $(R, +, \cdot)$ ein Ring und sei $r \in R$. Wir nennen r einen Nullteiler, falls ein $s \in R \setminus \{0\}$ existiert, sodass $r \cdot s = 0$.

Falls R keine Nullteiler besitzt, nennen wir R ein Integralsbereich.

Beispiel $(\mathbb{Z}, +, \cdot)$ ist ein Integralsbereich

$(\mathbb{Z}_{4\mathbb{Z}}, +, \cdot)$ ist kein Integralsbereich, weil $2 \cdot 2 = 4 \equiv 0 \pmod{4}$, d.h. $2 \in \mathbb{Z}_{4\mathbb{Z}}$ ist ein Nullteiler.

Lemma 112

Sei $r \in R^\times$, dann ist r kein Nullteiler.

Beweis

Angenommen $r \cdot s = 0$. Sei $r^{-1} \in R$ das Inverse zu, d.h. $r^{-1} \cdot r = 1$.

(r^{-1} kann als Linksinverses angenommen werden, weil R^\times eine Gruppe ist).

$\Rightarrow 0 = r \cdot s = r^{-1} \cdot r \cdot s = 1 \cdot s = s \Rightarrow r$ ist kein Nullteiler. \square

Wir haben im Beweis implizit Folgendes benutzt:

Lemma 113

$\forall r \in R: r \cdot 0 = 0$ und $0 \cdot r = 0$

Beweis

$$r \cdot 0 = r \cdot (0+0) = r \cdot 0 + r \cdot 0 \Rightarrow 0 = r \cdot 0.$$

↑
 $(R, +)$ ist eine Gruppe mit neutr. El. 0.

Analog für $0 \cdot r = 0$

□

Definition 114

Sei $(R, +, \cdot)$ ein Ring. Eine Teilmenge $I \subset R$ heißt **Ideal**, falls

- (1) $(I, +)$ eine Untergruppe von $(R, +)$ ist
- (2) $\forall r \in R: rI \subset I$ (d.h. $\forall r \in R$ und $s \in I$ ist $r \cdot s \in I$)
 und $Ir \subset I$ (d.h. $\forall r \in R$ und $s \in I$ ist $s \cdot r \in I$)

Bemerkung Definition 114 beschreibt ein **zweiseitiges Ideal**. Wir können linksseitige und rechtsseitige Ideale definieren.

In dieser Vorlesungen beschränken wir uns auf zweiseitige Ideale.

Lemma 115

Sei R ein Ring und $I, J \subset R$ Ideale. Dann sind auch folgende Mengen Ideale in R ,

$$(1) I \cap J$$

$$(2) I + J = \{ r+s \mid r \in I, s \in J \}$$

$$(3) I \cdot J = \left\{ \sum_{i=1}^n r_i \cdot s_i \mid r_i \in I, s_i \in J \text{ und } n \in \mathbb{N} \right\}$$

Beweis: Übung.

Definition 1.16

Sei R ein Ring und $I \subset R$ ein Ideal.

(1) Wir nennen I ein **Hauptideal**, falls ein $r \in R$ existiert mit

$$I = R \cdot r \cdot R = \left\{ \sum_{i=1}^n s_1^{(i)} \cdot r \cdot s_2^{(i)} \mid s_1^{(i)}, s_2^{(i)} \in R \right\}.$$

Wir schreiben: $I = (r)$

(2) Wir nennen I **endlich erzeugt**, falls es $r_1, r_m \in R$ gibt mit

$$I = (r_1) + \dots + (r_m)$$

Lemma 1.17

Sei R ein kommutativer Ring und $I = (r) \subset R$ ein Hauptideal. Dann hat I die Form:

$$I = r \cdot R = \{r \cdot s \mid s \in R\}.$$

Beweis

Es ist $(r) = RrR$. Sei $a = \sum_{i=1}^n s_1^{(i)} r \cdot s_2^{(i)} \in (r)$.

Dann ist auch $a = \sum_{i=1}^n r \cdot s_1^{(i)} \cdot s_2^{(i)} = r \sum_{i=1}^n s_1^{(i)} s_2^{(i)} \in r \cdot R$.

$$\Rightarrow (r) \subset r \cdot R.$$

Andererseits gilt $r \cdot R \subset (r)$ per Definition. □

Im Folgenden nehmen wir R als kommutativen Ring an.

Satz 118

$(\mathbb{Z}, +, \cdot)$ ist ein Hauptidealring

Beweis

Nach Lemma 43 sind alle Unterguppen von $(\mathbb{Z}, +)$ von der Form $m\mathbb{Z}$ für ein $m \in \mathbb{Z}$. □

Definition 119

Sei R ein Ring und $I \subset R$ ein Ideal. Wir nennen I

(1) ein maximales Ideal, falls für jedes Ideal J mit $I \subset J \subset R$ gilt: $I=J$ oder $R=J$.

(2) ein Primideal, falls $\forall r, s \in R$ gilt: $r \cdot s \in I \Rightarrow r \in I$ oder $s \in I$.

Lemma 120

(kommutativ)

Sei $\overset{\leftarrow}{R}$ ein Ring und I ein maximales Ideal in R , dann ist I prim.

Beweis

Seien $r, s \in R$ mit $r \cdot s \in I$. Es gibt zwei Fälle für $J = I + (r)$:

(1) $I=J$, dann ist $r \in I$ und wir sind fertig oder

(2) $J=R$.

Im zweiten Fall existiert $t \in R$, $m \in I$: $1 = m + tr$

$\Rightarrow s = s(m+tr) = s \cdot m + s \cdot t \cdot r \in I$, weil $s \cdot m \in I$ und

$\Rightarrow I$ ist ein Primideal.

$$s \cdot t \cdot r = t \cdot \frac{s \cdot r}{s} \in I$$

□

Restklasserringe

Sei R ein kommutativer Ring und $I \subset R$ ein Ideal.

Beobachtung R/I ist eine abelsche Gruppe bzgl. $+$, weil $I \subset R$ eine Untergruppe der kommutativen Gruppe $(R, +)$ und somit ein Normalteiler ist

Satz 121

$(R/I, +, \cdot)$ ist ein Ring mit der Multiplikation $(r+I)(s+I) = rs+I$.

Beweis

Es genügt zu zeigen, dass die Multiplikation von Restklassen wohldefiniert ist. Seien dazu $r+I$ und $s+I \in R/I$.

Dann ist:

$$\begin{aligned}
 (r+I) \cdot (s+I) &= \{(r+i_1)(s+i_2) \mid i_1, i_2 \in I\} \\
 &= \{r \cdot s + r \cdot i_2 + i_1 \cdot s + i_1 \cdot i_2 \mid i_1, i_2 \in I\} \\
 &= r \cdot s + I,
 \end{aligned}$$

weil $r \cdot i_2, i_1 \cdot s, i_1 \cdot i_2 \in I$ und I abgeschlossen bzgl. $+$ ist. \square

Satz 122

Sei R ein kommutativer Ring und $I \subset R$ ein Ideal.

- (1) Falls I maximal ist, ist R/I ein Körper
- (2) Falls I prim ist, ist R/I ein Integritätsbereich.

Beweis

Zu (1): Sei $r+I \in R/I$ mit $r+I \neq 0+I$, d.h. $r \notin I$.

Da I maximal ist und $r \notin I$ ist $I+(r) = R$.

Wir finden $m \in I$ und $t \in R$ mit $1 = mt + tr$.

$$\Rightarrow 1+I = t \cdot r + I = (t+I)(r+I)$$

$\Rightarrow r+I \in (R/I)^\times \Rightarrow R/I$ ist ein Körper.

Zu (2): Seien $r, s \in R \setminus I$ mit $(r+I)(s+I) = 0+I \in R/I$

$$\Rightarrow rs+I = 0+I = I \Rightarrow rs \in I.$$

I ist ein Primideal $\Rightarrow r \in I$ oder $s \in I$. Widerspruch zur Annahme, dass $r+I, s+I \neq 0+I \Rightarrow R/I$ ist ein Integritätsbereich. \square

Definition 123

Seien $(R, +_R, \cdot_R)$ und $(S, +_S, \cdot_S)$ zwei Ringe und

$\varphi: R \rightarrow S$ eine Abbildung. Wir nennen φ einen Ringhomomorphismus, falls

(1) $\varphi: (R, +_R) \rightarrow (S, +_S)$ einen Gruppenhomomorphismus ist

(2) $\forall r, s \in R: \varphi(r \cdot_R s) = \varphi(r) \cdot_S \varphi(s)$

Bemerkung

Falls R, S Körper sind ist ein Ringhomomorphismus $\varphi: R \rightarrow S$ ein Körperhomomorphismus im Sinne von Definition 75.

Satz 124

Seien R, S kommutative Ringe und $\varphi: R \rightarrow S$ ein Ringhomomorphismus.

Dann gilt:

- (1) $\varphi(R) \subset S$ ist ein Unterring
 - (2) $\ker(\varphi) = \{ r \in R \mid \varphi(r) = 0 \in S \}$ ist ein Ideal in R
 - (3) $\frac{R}{\ker(\varphi)} \cong \varphi(R)$ (Homomorphiesatz)
- ↑
(d.h. es existiert ein bijektiver Ringhom.
zwischen $\frac{R}{\ker(\varphi)}$ und $\varphi(R)$)

Beweis

Analog zum Gruppenfall.

Bemerkung

Kern von Ringhomomorphismen sind Ideale und Ideale sind Kern von Ringhomomorphismen (d.h. $I = \ker(\varphi)$, für $\varphi: R \rightarrow R/I$, $r \mapsto r+I$)

Lemma 125

Sei $f \in K[x]$ ein irreduzibles Polynom, wobei $Q \subseteq K \subseteq \mathbb{C}$ ein Körper ist.

Dann ist (f) ein maximales Ideal.

Beweis

Angenommen wir finden ein Ideal J mit $(f) \subset J \subset K[x]$. Sei $g \in J$ ein Polynom vom kleinsten Grad in J .

Behauptung $J = (g)$.

Beweis Sei $h \in J$, dann betrachten wir Polynomdivision:

$$h = g \cdot s + r \quad \text{mit } s \in K[x] \text{ und } r \in K[x] \text{ mit} \\ \deg(r) < \deg(g).$$

Es gilt: $r = h - g \cdot s \in J$, da $h \in J$ und $g \in J \Rightarrow r = 0$
 $\Rightarrow h = g \cdot s \Rightarrow h \in (g)$.

Da $(f) \subset (g) = J$, folgt, dass $f = g \cdot s$ für ein $s \in K[x]$.

Weil f irreduzibel ist, folgt, dass $s \in K^\times$ und somit $s \in (K[x])^\times$
 $\Rightarrow (f) = (g)$ (weil $g = s^{-1} \cdot f$). \square

Korollar 126

$K[x]$ ist ein Hauptidealring (d.h. alle Ideale in $K[x]$ sind Hauptideale).

Korollar 127

Sei $f \in K[x]$ irreduzibel. Dann ist

(1) $K[x]/(f)$ ist ein Körper

(2) Falls α eine Nullstelle von f ist, so ist

$$K[x]/(f) \cong K(\alpha).$$

Beweis

(1) ist eine Kombination aus Satz 122 und Satz 125

(2) Betrachte den Ringhomomorphismus $\varphi: K[x] \rightarrow K(\alpha)$, $g \mapsto g(\alpha)$.
 $\ker(\varphi) = (f)$, weil $\ker(\varphi) = \{g \in K[x] \mid g(\alpha) = 0\}$,

und weil f das Minimalpolynom von α ist.

$$\Rightarrow K[x]/(f) \cong \{g(K[x]) \mid g \in K[x]\} \quad (*)$$

Andererseits ist $K[x]/(f)$ ein Körper, d.h. $\varphi(K[x])$ ist ein Körper

$$\Rightarrow \varphi(K[x]) = K(\alpha)$$

$$\Rightarrow K[x]/(f) \cong K(\alpha).$$

□

Bemerkung (1) Die Gleichung (*) liefert einen strukturellen Beweis für die Bemerkung nach Satz 70, nämlich dass

$$K(\alpha) = \{g(\alpha) \mid g \in K[x], \deg(g) < \deg(f)\},$$

wobei f das Minimalpolynom von α ist.

(2) Korollar 127 zeigt, wie wir auf dem Computer in $K(\alpha)$ rechnen können. Wir rechnen in $K[x]$ und stellen die Elemente in $K(\alpha)$ als Restklassen in $K[x]/(f)$ dar (f ist das Minimalpolynom von α).

Beispiel: Seien $x, y \in K(\alpha)$. Wie berechnen wir $x \cdot y$?

1. Schreibe dar $x = g(\alpha), y = h(\alpha)$.

2. Berechne $g \cdot h \in K[x]$.

3. Finde $p \in K[x]$ mit $\deg(p) < \deg(f)$ und
 $p + (f) = g \cdot h + (f)$

mit Polynomdivision.

4. $x \cdot y = p(\alpha)$.