

1. Script zur Vorlesung: Algebra (B III)

Prof. Dr. Salma Kuhlmann, Dr. Lorna Gregory, Katharina Dupont

WS 2012/2013: 22. Oktober 2012

Kapitel 1

Faktorringe, Homomorphismen, Ideale, Ringe von Brüchen, Quotientenkörper,
Lokalisierung, Chinesischer Reste-Satz, Euklidische und Hauptideal Ringe,
Faktorielle Ringe, Polynom-Ringe, Irreduzibilitätskriterien

Alle Ringe in dieser Vorlesung sind kommutativ mit $1 \neq 0$.

Erinnerungen

Sei R ein Ring.

- (1) $a \neq 0; a \in R$ ist ein *Nullteiler*, wenn es $b \neq 0; b \in R$ gibt mit $ab = 0$.
- (2) R ist ein *Integerring* oder *Integritätsbereich*, wenn er keine Nullteiler hat.
- (3) Ein endlicher Integritätsbereich ist ein Körper (siehe Übungsblatt 1, Aufgabe 1.4 (b)).
- (4) $u \in R$ ist eine *Einheit*, wenn es ein $v \in R$ gibt mit $uv = 1$.

Notation: $R^\times :=$ Menge der Einheiten von R .

Proposition

R^\times ist eine multiplikative Gruppe.

Beispiele

$\mathbb{Z}_n^\times = U(n)$ (Übungsblatt 3, Aufgabe 2b aus Lineare Algebra 1)

$a \in U(n) \Leftrightarrow \text{ggT}(a, n) = 1$.

Euler φ -Funktion: $\varphi : \mathbb{N} \rightarrow \mathbb{N}$

$\varphi(n) := |U(n)|$.

Siehe Übungsblatt für eine ausführliche Ausarbeitung der Eigenschaften von φ :

- (1) $\varphi(p^v) = p^v - p^{v-1}$ für p Primzahl und $v \in \mathbb{N}$
- (2) φ ist eine multiplikative arithmetische Funktion i.e. $\varphi(ab) = \varphi(a)\varphi(b)$,
wenn $\text{ggT}(a, b) = 1$.

Definition

(1) $S \subseteq R$ ist ein *Teiltring*, wenn $S \neq \emptyset$; $a, b \in S \Rightarrow a - b \in S$ und $ab \in S$.

(2) Seien R, S Ringe. $\varphi : R \rightarrow S$ ist ein *Ringhomomorphismus*, wenn
 $\varphi(1_R) = 1_S$, $\varphi(a + b) = \varphi(a) + \varphi(b)$, $\varphi(ab) = \varphi(a)\varphi(b)$.

Notation:

$$\ker \varphi := \{x \in R; \varphi(x) = 0\}$$

$$\text{im } \varphi := \{y \in S; \exists x \in R \text{ mit } \varphi(x) = y\} := \varphi(R).$$

(3) Ein *Ringisomorphismus* ist ein bijektiver Ringhomomorphismus.

Notation: $\varphi : R \simeq S$ oder $R \xrightarrow{\varphi} S$ oder $R \simeq S$.

Bemerkung

Sei φ ein Homomorphismus: φ ist injektiv $\Leftrightarrow \ker \varphi = \{0\}$.

Beispiel

Sei $n \in \mathbb{N}$

Notation

$a \in \mathbb{Z}; \bar{a} := \text{Rest nach Division durch } n$.

$$\varphi : \mathbb{Z} \rightarrow \mathbb{Z}_n$$

$$a \mapsto \bar{a}$$

ist ein Ringhomomorphismus mit $\ker \varphi = \{nz/z \in \mathbb{Z}\} := n\mathbb{Z}$

(siehe Lineare Algebra 1, 2. Vorlesung).

Definition

Ein Teilring $I \subseteq R$ ist ein *Ideal*, wenn aus $r \in R$ und $x \in I$ folgt: $rx \in I$.

Notation: $I \triangleleft R$

Beispiele

$$I = R \quad \text{und} \quad I = \{0\}$$

Terminologie

$I \triangleleft R$ und $I \neq R$ heißt *echtes Ideal*.

$I \triangleleft R$ und $I \neq \{0\}$ heißt *nicht triviales Ideal*.

Proposition

Sei $\varphi : R \rightarrow S$ ein Ringhomomorphismus. Es gelten:

(1) $\text{im } \varphi$ ist ein Teilring von S .

(2) $\ker \varphi$ ist ein Ideal von R .

Faktoring

Sei $I \triangleleft R$. $R/I := \{x + I \mid x \in R\}$ die Menge der *Nebenklassen von R modulo I* (siehe Übungsblatt 1, Aufgabe 1.2) (also der Äquivalenzklassen $[x]$ bezüglich $x \sim y \pmod I$ genau dann, wenn $x - y \in I$).

Proposition

R/I ist ein Ring mit den Ringoperationen

$$(r + I) + (s + I) := (r + s) + I \text{ und}$$

$$(r + I) \cdot (s + I) := (rs) + I$$

für alle $r, s \in R$ (Übungsblatt 1, Aufgabe 1.2).

Definition

R/I ist der *Faktoring* " R modulo I ".

Satz (Isomorphiesatz für Ringe)

(1) Sei $\varphi : R \rightarrow S$ ein Ringhomomorphismus. Es gilt $R / \ker \varphi \simeq \text{im } \varphi$.

(2) Umgekehrt: Ist $I \triangleleft R$, dann ist

$$\pi : R \rightarrow R/I$$

$$r \mapsto r + I$$

ein surjektiver Ringhomomorphismus mit $\ker \pi = I$ (π ist die *kanonische Projektion*).

Also sind die Ideale genau die Kerne von Ringhomomorphismen.

Beweis

Behauptung die Abbildung von (1)

$$\Phi : R/I \rightarrow \varphi(R)$$

$$x + I \mapsto \varphi(x)$$

ist wohldefiniert (i.e. $x + I = y + I$ impliziert $\varphi(x) = \varphi(y)$).

Es ist klar, dass Φ surjektiv und ein Ringhomomorphismus ist. Wir berechnen $\ker \Phi$.

$$\Phi(x + I) = 0 \Leftrightarrow \varphi(x) = 0 \Leftrightarrow x \in \ker \varphi \Leftrightarrow x \in I \Leftrightarrow x + I = 0 + I;$$

somit ist $\ker \Phi = \{0 + I\}$ (das Nullelement der Faktoring R/I).

Beweis von (2) analog. □

Beispiel

$$\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}_n$$

Korollar 1

Sei $I \triangleleft R, J \triangleleft R$ mit $I \subseteq J$ (insbesondere $I \triangleleft J$). Dann ist $J/I \triangleleft R/I$ und $(R/I)/(J/I) \simeq R/J$.

Beweis

Die Abbildung

$$\begin{aligned} \Phi : R/I &\rightarrow R/J \\ x + I &\mapsto x + J \end{aligned}$$

ist ein surjektiver Ringhomomorphismus mit $\ker \Phi = J/I$.

□