→ Algebra (B III). ←

→ WS 2012 - 2013. ←

→ Kuhlmann ←

Inhalt und (voraussichliche) Terminplanung.

Kapitel I: Ringe, 7 Vorlesungen 22.10 - 15.11

Kapitel II: Körpererweiterungen, 6 Vorlesungen 15.11 - 10.12

Kapitel III: Gruppen, 7 Vorlesungen 10.12 - 17.01

Kapitel IV: Galoistheorie, 8 Vorlesungen 17.01 - 14.02

Kapitel I:

Inhalt im Stichpunkten $:=$ Faktorringe, Homomorphismen, Ideale, Ringe von Brüchen, Quotientenkörper, Lokalisierung, Chinesischer Reste Satz, Euklidische und Hauptideal Ringe, Faktorielle Ringe, Polynomringe, Irreduzibilitätskriterien.

---

1. Vorlesung.

am 22. 10. 2012.

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

Erinnerungen. Sei R ein Ring.

1. $a \neq 0$; $a \in R$ ist Nullteiler wenn es $b \neq 0$, $b \in R$ gibt mit $ab = 0$.

2. R ist Integerring oder Integritätsbereich wenn er keine Nullteiler hat.

3. Ein endlicher Integritätsbereich ist ein Körper. ∎ Siehe [ÜB 1 Auf 1.4 (b)].

4. $u \in R$ ist eine Einheit wenn $\exists v \in R$ mit $uv = 1$.

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

Proposition. $R^{\times}$ ist eine multiplikative Gruppe. ∎

Beispiele. $\mathbb{Z}_n^{\times} = \mathcal{U}(n)$ (Zettel 3 Auf. 2b LA I)

$a \in U(n) \iff ggT(a, n) = 1.$

Euler φ- Funktion

$$\varphi : \mathbb{N} \longrightarrow \mathbb{N}$$

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

Siehe ÜB für eine ausführliche Ausarbeitung der Eigenschaften von φ:

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

<u>Definition</u> (1) $S \subseteq R$ ist <u>Teilring</u> wenn:

$S \neq \emptyset$; $a, b \in S \Rightarrow a - b \in S$ und $ab \in S$.

Seien R, S Ringe.

(2) $\varphi : R \longrightarrow S$ ist <u>Ringhomomorphismus</u> wenn

$$\varphi(1_R) = 1_S, \quad \varphi(a+b) = \varphi(a) + \varphi(b), \quad \varphi(ab) = \varphi(a)\varphi(b).$$

<u>Notation</u>. $\ker \varphi := \{x \in R ; \ \varphi(x) = 0\}$

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

$:= \varphi(R).$

(3) Ein Ringisomorphismus ist ein bijektiver Ringhomomorphismus.

Notation $\varphi : R \simeq S$ oder

$R \overset{\varphi}{\simeq} S$

oder $R \simeq S$.

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

—— // ——

Beispiel. Sei $n \in \mathbb{N}$. Notation. $a \in \mathbb{Z}$; $\bar{a} :=$ Rest nach Division durch n.

$$\varphi : \mathbb{Z} \longrightarrow \mathbb{Z}_n$$
$$a \longmapsto \bar{a}$$

ist Ringhomo. mit $\ker\varphi = \{nz \mid z \in \mathbb{Z}\} := n\mathbb{Z}$

(siehe LA I 2. Vorlesung). $\square$

—— // ——

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

Notation. $I \trianglelefteq R$.

Beispiele $I = R$ und $I = \{0\}$

Terminologie: $I \trianglelefteq R$ und $I \neq R$

heißt: <u>echtes</u> <u>Ideal</u>.

$I \trianglelefteq R$ und $I \neq \{0\}$

heißt: <u>nicht</u> <u>triviales</u> <u>Ideal</u>.

Proposition: Sei $\varphi : R \longrightarrow S$ Ringhomo.
Es gelten:

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

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

Faktorring. Sei $I \trianglelefteq R$

$R/I := \{x + I \mid x \in R\}$ die Menge

der <u>Nebenklassen von R modulo I</u>.

(siehe ÜB 1 Auf. 1.2)

(also der Äquivalenzklassen $[x]$ bezüglich:
$x \sim y \mod I$ gdw $x - y \in I$.) $\blacksquare$

Proposition.

R/I ist ein Ring, mit den Ringoperationen:

$(r+I) + (s+I) := (r+s) + I$ und

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

$\forall\, r, s \in R$. (ÜB 1 Auf. 1.2) $\square$

Definition R/I ist der <u>Faktorring</u>

"<u>R modulo I</u>".

Satz (Isomorphiesatz für Ringe).

(1) Sei $\varphi: R \to S$ Ringhomo, es gilt

$$R/_{\ker\varphi} \cong \operatorname{im}\varphi.$$

(2) umgekehrt: ist $I \trianglelefteq R$ dann ist

$$\begin{aligned} \pi: R &\longrightarrow R/I \\ r &\longmapsto r+I \end{aligned}$$

ein surjektiver Ringhomo. mit $\ker\pi = I$.

(π ist die <u>kanonische</u> <u>Projektion</u>).

* Also sind die Ideale genau die Kerne von Ringhomo. *.

Beweis: Beh. die Abbildung von (1).

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

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

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

Es ist klar daß Φ surjektiv ist, und ein Ringhomo..

Wir berechnen $\ker \Phi$.

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

$\iff x \in I \iff x+I = 0+I$,

somit ist $\ker \Phi = \{0+I\}$

das Nullelement der Faktorring R/I. ∎

Beweis von (2) ist analog. ∎∎

Beispiel:

$$\mathbb{Z}/_{n\mathbb{Z}} \cong \mathbb{Z}_n. \qquad \blacksquare$$

— " —

Korollar:

Sei $I \trianglelefteq R$, $J \trianglelefteq R$ mit

$$I \subseteq J \qquad (\text{insbesondere } I \trianglelefteq J).$$

Dann ist $J/_I \trianglelefteq R/I$ und

$$(R/I)\big/_{(J/I)} \cong R/J.$$

Beweis. die Abbildung

$$\Phi : R/_I \twoheadrightarrow R/J$$
$$x + I \longmapsto x + J$$

ist ein surjektiver Ringhomo. mit

$$\ker \Phi = J/I. \qquad \blacksquare$$