§ 3 Kommutative Ringe

1. Def Ein Ring $(R, +, \cdot, 0, 1)$ besteht aus einer Menge R mit zwei Verknüpfungen $+, \cdot$ sowie Elementen $0, 1 \in R$ so, dass gilt:

(R1) $(R, +)$ ist eine abelsche Gruppe mit 0 als Neutralelement

(R2) $(R, \cdot)$ ist ein Monoid mit 1 als Neutralelement (d.h. die Verknüpfung ist assoziativ und $a \cdot 1 = 1 \cdot a = a$ gilt für alle $a \in R$)

(R3) Es gelten die Distributivgesetze
$a(b+c) = ab + ac \qquad (a+b)c = ac + bc$.

Wenn zusätzlich gilt $ab = ba$ für alle $a, b \in R$, so heißt R ein kommutativer Ring. Konvention wie in der Schule: Punkt vor Strich, also $ab + c = (a \cdot b) + c$ usw.

Ein Element $a \in R$ heißt Einheit, wenn es $b \in R$ gibt mit $ab = 1 = ba$. Die Einheiten bilden eine Gruppe $R^\times = \{ a \in R \mid a \text{ Einheit} \}$, denn:

$1 \in R^\times$, $a, b \in R^\times \Rightarrow ab \in R^\times$ ($a\tilde{a} = \tilde{a}a = 1$, $b\tilde{b} = \tilde{b}b = 1$)

$\Rightarrow ab\,\tilde{b}\tilde{a} = 1 = \tilde{b}\tilde{a}ab$. Ist also $a \in R^\times$, so hat a ein eindeutig bestimmtes multiplikatives Inverses $a^{-1} \in R^\times$.

Beispiele (a) $\mathbb{R}, \mathbb{Q}, \mathbb{Z}, \mathbb{C}$ sind kommutative Ringe, $\mathbb{R}^\times = \mathbb{R} - \{0\}$, $\mathbb{Z}^\times = \{\pm 1\}$
Körper sind Ringe.

(b) V ein Vektorraum über einem Körper K,
$R = End(V) = \{ f : V \to V \mid f \text{ linear} \}$ ist ein Ring, nicht kommutativ für $\dim(V) \geq 2$, $R^\times = GL(V)$

(c) $R = \{0\}$ ist ein Ring mit $1 = 0$, $0 \cdot 0 = 0 = 0 + 0$, der Nullring. Hier ist $R = R^\times$!

2. Rechenregeln in Ringen.

(i) Additiv darf man kürzen: $a + x = a + y \Rightarrow x = y$

(ii) es gilt $a \cdot 0 = 0 \cdot a = 0$ für alle $a \in R$

(iii) $a(-b) = -ab = (-a)b$ für alle $a, b \in R$
insbesondere $(-1)a = -a$ und $(-a)(-b) = ab$

Beweis (i) klar, denn $(R, +)$ ist eine Gruppe

(ii) $a \cdot 0 = a(0+0) = a \cdot 0 + a \cdot 0 \Rightarrow a \cdot 0 = 0$ usw

(iii) $a(-b) + ab = a(-b+b) = a \cdot 0 = 0 \Rightarrow a(-b) = -ab$
ferner $(-a)b = -ab$
$(-a)(-b) = -(-a)b = -(-ab) = ab$ □

Vorsicht: Multiplikativ darf man nicht immer kürzen. Bsp $R = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{R} \right\}$ Matrizenring

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$
$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

3. Homomorphismen und Ideale

Seien R, S Ringe.

Ein Abbildung $\varphi: R \to S$ heißt Ringhomomorphismus, wenn für alle $a, b \in R$ gilt:

(RH1) $\varphi(a+b) = \varphi(a) + \varphi(b)$

(RH2) $\varphi(ab) = \varphi(a)\varphi(b)$

(RH3) $\varphi(1_R) = 1_S$

Der Kern eines Ringhomomorphismus ist $\ker(\varphi) = \{a \in R \mid \varphi(a) = 0\}$.

Ein Teilmenge $I \subseteq R$ heißt Ideal in Ring R, wenn gilt

(I1) $(I, +)$ ist Untergruppe von $(R, +)$

(I2) Für alle $j \in I$, $a \in R$ gilt $ja, aj \in I$

(I absorbiert R)

Wir schreiben dann $I \trianglelefteq R$.

Lemma Der Kern eines Ringhomomorphismus ist ein Ideal.

Beweis Sei $\varphi: R \to S$ ein Ringhomomorphismus, sei $I = \ker(\varphi) = \{a \in R \mid \varphi(a) = 0\}$. Dann ist $I \subseteq R$ ein Untergruppe bzgl. Addition. Für $j \in I$, $a \in R$ gilt $\varphi(aj) = \varphi(a)\varphi(j) = 0 = \ldots = \varphi(ja)$

$\Rightarrow ja, aj \in I$ und $I \trianglelefteq R$. □

4 Konstruktion: Quotienten Sei I ein Ideal im Ring R. Dann ist $R/I = \{ a+I \mid a \in R \}$ ein Ring. Wir definieren eine Verknüpfung auf R/I durch $(a+I)(b+I) = ab+I$

Das ist wohldefiniert: $\left.\begin{array}{l} a+I = \tilde{a}+I \\ b+I = \tilde{b}+I \end{array}\right\} \Rightarrow \begin{array}{l} \tilde{a} = a+i \\ \tilde{b} = b+j \end{array}$

für $i,j \in I$ $\quad \tilde{a}\tilde{b}+I = (a+i)(b+j)+I = ab + \underbrace{ib+aj+ij}_{\in I} + I$

$= ab+I$. Diese Verknüpfung ist dann assoziativ, und $1+I$ ist ein Neutralelement.

Folglich ist R/I wieder ein Ring. Die Abbildung $p_I : R \to R/I$, $a \longmapsto a+I$ ist ein Ringhomomorphismus mit $\ker I = \ker(p_I)$.

Fazit Ist R ein Ring, so sind die Ideale in R genau die Kerne von Ringhomomorphismen.

Beobachtung Sei $I \trianglelefteq R$ ein Ideal. Falls gilt $I \cap R^\times \neq \{0\}$, so ist $I = R$.

Denn: $a \in I \cap R^\times \Rightarrow$ es gibt $\tilde{a} \in R$ mit $a\tilde{a} = 1$

$\Rightarrow 1 \in I \Rightarrow$ für jedes $b \in R$ ist $b = b1 \in I$. ⊏7

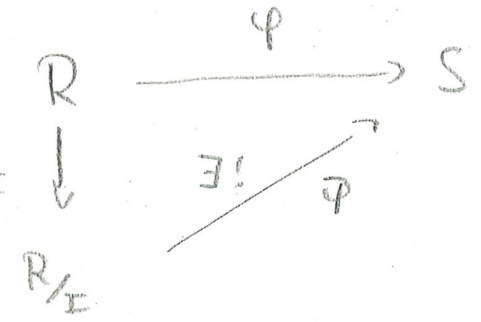
Insbesondere: Ist R ein Körper, so sind $\{0\}$ und R die einzigen Ideale in R.

5. Lemma Die Ideale im Ring $\mathbb{Z}$ sind genau die Mengen $m\mathbb{Z}$, für $m \in \mathbb{N} = \{0,1,2,\dots\}$.

Beis. Für jedes $m \in \mathbb{N}$ ist $m\mathbb{Z}$ ein Ideal, denn $m\mathbb{Z}$ ist Untergruppe von $(\mathbb{Z},+)$ und für $a = mk \in m\mathbb{Z}$, $b \in \mathbb{Z}$ ist $ab = mkb \in m\mathbb{Z}$.

Sei $I \trianglelefteq \mathbb{Z}$ ein Ideal. $I = \{0\}$ o.k. Sonst $I \neq \{0\}$, wähle $m \in I$ so, dass $m > 0$ minimal ist. (Das geht, denn $\mathbb{N} \subseteq \mathbb{Z}$ ist wohlgeordnet!) Es folgt $m\mathbb{Z} \subseteq I$. Ist $a \in I$ so setze $a = m \cdot k + r$, $0 \leq r < m$ so $r \in I$ so $r = 0$, also $I = m\mathbb{Z}$. □

6. Satz (Homomorphiesatz) Sei $\varphi: R \to S$ ein Homomorphismus von Ringen, sei $I \trianglelefteq R$ ein Ideal mit $I \subseteq \ker(\varphi)$, sei $p_I : R \to R/I$ der kanonische Homomorphismus $a \mapsto a+I$. Dann gibt es genau ein Ringhomomorphismus $\overline{\varphi}: R/I \to S$ mit $\overline{\varphi} \circ p_I = \varphi$



Beis. Aus dem Homomorphiesatz für Gruppen § 1.19 folgt: es gibt genau einen Gruppenhomomorphismus $\overline{\varphi}$ mit $\overline{\varphi} \circ p_I = \varphi$, und $\overline{\varphi}(a+I) = \varphi(a)$.