Definition (11.1)

Sei R ein Ring, I ein Ideal und $a \in R$. Dann nennen wir die Menge

$$a + I \quad = \quad \{a + i \mid i \in I\}$$

die Nebenklasse von a modulo I. Die Menge $\{a + I \mid a \in R\}$ aller Nebenklassen von Elementen aus R bezeichnen wir mit R/I.

Die Kongruenzrelation modulo eines Ideals

Proposition (11.2)

Sei R ein Ring und I ein Ideal. Dann ist die Relation auf R gegeben durch

$$a \equiv b \mod I \quad \Leftrightarrow \quad b - a \in I$$

eine Äquivalenzrelation, und die Elemente von R/I sind genau die Äquivalenzklassen dieser Relation. Man spricht in diesem Zusammenhang von einer Kongruenzrelation und bezeichnet zwei Elemente a, b derselben Äquivalenzklasse als kongruent modulo I.

Beweis von Proposition 11.2

geg.: Ring R, Ideal I in R

$$a \equiv b \mod I \iff b-a \in I$$

<u>Beh</u>.: (1) $\equiv$ ist eine Äquivalenzrelation

(2) Die Äquivalenzklassen der Relation sind genau die Elemente von $a+I$.

<u>zu (1)</u> Seien $a, b, c \in R$

Reflexivität: $0_R \in I$ (da I Ideal) $\Rightarrow a-a \in I$

$\Rightarrow a \equiv a \mod I$

Symmetrie: Setze $a \equiv b \mod I$ voraus. $\Rightarrow b-a \in I$

$\overset{I \text{ Ideal}}{\Longrightarrow} (-1_R)(b-a) \in I \Rightarrow a-b \in I \Rightarrow b \equiv a \mod I$

Transitivität: Setze $a \equiv b \mod I$ und $b \equiv c \mod I$

$\Rightarrow b-a \in I$ und $c-b \in I \overset{I \text{ Ideal}}{\Longrightarrow} (b-a)+(c-b) \in I$

$\Rightarrow c-a \in I \Rightarrow a \equiv c \mod I$

zu (2) Sei $a \in R$ und $[a]$ die Äquivalenzklasse von a bzgl der Relation $\equiv$. Dann gilt für jedes $b \in R$ die Äquivalenz $b \in [a] \Leftrightarrow a \equiv b \mod I \Leftrightarrow b-a \in I$

$\Leftrightarrow \exists\, i \in I : b-a = i \Leftrightarrow \exists\, i \in I : b = a+i$

$\Leftrightarrow b \in a+I$.

Also gilt $[a] = a+I$. $\square$

Wichtige Rechenregel für Kongruenzklassen

Nach Definition sind zwei Elemente $a, b \in R$ also genau dann kongruent modulo I, wenn ihre Kongruenzklassen übereinstimmen. Da je zwei Äquivalenzklassen entweder disjunkt oder gleich sind, erhalten wir die Äquivalenz

$$a \equiv b \mod I \quad \Leftrightarrow \quad b - a \in I \quad \Leftrightarrow \quad a + I = b + I \quad \Leftrightarrow \quad b \in a + I.$$

Die Elemente des Restklassenrings $\mathbb{Z}/n\mathbb{Z}$

Proposition (11.3)

Die Menge $\mathbb{Z}/n\mathbb{Z}$ der Kongruenzklassen ist n-elementig, es gilt

$$\mathbb{Z}/n\mathbb{Z} \quad = \quad \{\bar{a} \mid a \in \mathbb{Z}\ ,\ 0 \le a < n\}.$$

Gleichbedeutend damit ist die Feststellung, dass die Elemente der Menge $\{0, 1, ..., n-1\}$ ein Repräsentantensystem von $\mathbb{Z}/n\mathbb{Z}$ bildet.

Proposition (11.4)

Sei K ein Körper, $R = K[x]$ und $f \in K[x]$ ein Polynom vom Grad $n \geq 1$. Dann ist die Teilmenge

$$S = \{g \in K[x] \mid g \neq 0, \mathrm{grad}(g) < n\} \cup \{0\}$$

von $K[x]$ ein Repräsentantensystem von $R/(f)$.

Erinnerung:

Sei R ein Ring. Dann ist der Polynomring $R[x]$ über R ein Erweiterungsring von R mit folgender Eigenschaft: Für jedes $f \in R[x] \setminus \{0_R\}$ gibt es *eindeutig bestimmte* $n \in \mathbb{N}_0$ und $a_0, a_1, \ldots, a_n \in R$, $a_n \neq 0_R$, so dass

$$f = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$$

gilt. Man nennt n den *Grad* von f (Bezeichnung $\operatorname{grad}(f)$), und a_n den *Leitkoeffizienten* von f, $a_n x^n$ den *Leitterm*.

wichtig: Es gilt $x \notin R$.

Beispiel zu Proposition 11.4:

Die Menge $S = \{a + bx \mid a, b \in \mathbb{R}\}$ ist ein Repräsentantensystem von $\mathbb{R}[x]/(x^2+1)$.

Beweis von Proposition 11.4:

geg.: K Körper, $f \in K[x] \setminus K$, $n = \text{grad}(f)$

$S = \{g \in K[x] \mid \text{grad}(g) < n\} \cup \{0_K\}$

z.zg.: Jede Nebenklasse in $K[x]/(f)$ enthält genau ein Element aus S.

Sei $g \in K[x]$ vorgegeben. Wir zeigen:

(1) $g + (f)$ enthält ein Element aus S

(2) $g + (f)$ enthält nicht mehr als ein Element aus S

<u>zu(1)</u> Division mit Rest $\Rightarrow \exists\, q, r \in K[x]$ mit $g = qf + r$ und $r = 0$ oder $\operatorname{grad}(r) < \operatorname{grad}(f)$, d.h. $r \in S$. Es gilt $r = g + (-q)f \Rightarrow r \in g + (f)$

<u>zu(2)</u> Seien $r_1, r_2 \in S$ mit $r_1, r_2 \in g + (f)$.

zzg: $r_1 = r_2$ $\quad r_1, r_2 \in g + (f) \Rightarrow \exists\, q_1, q_2 \in K[x]$ mit $r_1 = g + q_1 f$, $r_2 = g + q_2 f \Rightarrow r_2 - r_1 = (g + q_2 f) - (g + q_1 f) = (q_2 - q_1) f$ $\quad r_1, r_2 \in S \Rightarrow$ $r_2 - r_1 = 0$ oder $\operatorname{grad}(r_2 - r_1) < n$, $\operatorname{grad}(f) = n$

$\underset{\Longrightarrow}{f \mid (r_2 - r_1)}$ $\quad r_2 - r_1 = 0_K \Rightarrow r_1 = r_2$ $\quad \square$

Addition und Multiplikation auf Nebenklassen

Proposition (11.5)

Sei R ein Ring und I ein Ideal. Dann gibt es (eindeutig bestimmte) Verknüpfungen $+$ und $\cdot$ auf R/I mit der Eigenschaft

$$(a+I)+(b+I)=(a+b)+I \quad \text{und} \quad (a+I)\cdot(b+I)=ab+I$$

für alle $a, b \in R$.

Beweis von Proposition 11.5:

Wir verwenden Satz 4.25, um die Existenz der Verknüpfungen $+$ und $\cdot$ auf R/I nachzuweisen. Dafür muss gezeigt werden:

Für alle $a, a', b, b' \in R$ folgt aus

$a \equiv a' \mod I$ und $b \equiv b' \mod I$ $(*)$

jeweils $(a+b)+I = (a'+b')+I$ und

$$ab + I = a'b' + I$$

Seien also $a, a', b, b' \in I$ mit $(*)$ vorgeg. Dann gilt $i = a' - a \in I$

und $j = b' - b \in I$.

zur Addition z.zg.: $(b'+a') - (b+a) \in I$

Dies ist erfüllt, da $(b'+a') - (b+a) = (b'-b) + (a'-a)$
$= j + i \in I$.

zur Multiplikation: z.zg.: $a'b' - ab \in I$

Es gilt $a'b' - ab = a'b' - ab' + ab' - ab =$
$(a'-a) \cdot b' + a(b'-b) = b'(a'-a) + a(b'-b) =$
$\underbrace{b'i}_{\in I} + \underbrace{aj}_{\in I} \in I$. $\square$

Existenz des Faktorrings

Satz (11.6)

Sei R ein Ring und $I \subseteq R$ ein Ideal. Dann ist R/I mit den beiden soeben definierten Verknüpfungen ein Ring, den man als Faktorring bezeichnet. Die Abbildung $\pi_I : R \to R/I$ gegeben $a \mapsto a + I$ ist ein Epimorphismus von Ringen, der sog. kanonische Epimorphismus.

$x^2 - (-1) = x^2 + 1 \in (f)$

Anwendungsbeispiele:

(1) ein Körper mit vier Elementen (nicht $\mathbb{Z}/4\mathbb{Z}$)

Sei $K = \mathbb{F}_2[x]/(f)$ mit $f = x^2 + x + \bar{1} \in \mathbb{F}_2[x]$.

Es gilt $K = \{\bar{0} + (f), \bar{1} + (f), x + (f), \bar{1} + x + (f)\}$.

Beispiel für eine Addition:

$$(x + (f)) + (x + \bar{1} + (f)) = \bar{1} + \bar{2} \cdot x + (f) = \bar{1} + (f)$$

Beispiel für eine Multiplikation:

zu beachten: $x^2 + (f) = \bar{1} + x + (f)$, wegen

$$x^2 - (\bar{1} + x) = x^2 - x - \bar{1} \underset{[\bar{1} = -\bar{1} \text{ in } \mathbb{F}_2]}{=} x^2 + x + \bar{1} = f \in (f)$$

$$(x + (f)) \cdot (\bar{1} + x + (f)) = x \cdot (\bar{1} + x) + (f) = x + x^2 + (f)$$

$$x+(f)\cdot x^2+(f) \overset{s.o.}{=} x+(f)\cdot \bar{1}+x+(f) =$$
$$\bar{1}+\bar{2}\cdot x+(f) = \bar{1}+(f) = 1_K \Rightarrow (x+(f))^{-1} = \bar{1}+x+(f)$$

Verknüpfungstabelle der Addition

$+$	$\bar{0}+(f)$	$\bar{1}+(f)$	$x+(f)$	$\bar{1}+x+(f)$
$\bar{0}+(f)$	$\bar{0}+(f)$	$\bar{1}+(f)$	$x+(f)$	$\bar{1}+x+(f)$
$\bar{1}+(f)$	$\bar{1}+(f)$	$\bar{0}+(f)$	$\bar{1}+x+(f)$	$x+(f)$
$x+(f)$	$x+(f)$	$1+x+(f)$	$\bar{0}+(f)$	$\bar{1}+(f)$
$\bar{1}+x+(f)$	$\bar{1}+x+(f)$	$x+(f)$	$\bar{1}+(f)$	$\bar{0}+(f)$

Verkn.-tab. der Multiplikation

$\cdot$	$\bar{0}+(f)$	$\bar{1}+(f)$	$x+(f)$	$\bar{1}+x+(f)$
$\bar{0}+(f)$	$\bar{0}+(f)$	$\bar{0}+(f)$	$\bar{0}+(f)$	$\bar{0}+(f)$
$\bar{1}+(f)$	$\bar{0}+(f)$	$\bar{1}+(f)$	$x+(f)$	$\bar{1}+x+(f)$
$x+(f)$	$\bar{0}+(f)$	$x+(f)$	$\bar{1}+x+(f)$	$\bar{1}+(f)$
$\bar{1}+x+(f)$	$\bar{0}+(f)$	$\bar{1}+x+(f)$	$\bar{1}+(f)$	$x+(f)$

(2) Konstruktion der komplexen Zahlen (vorläufig)

Definiere $\mathbb{C} = \mathbb{R}[x]/(x^2+1)$, $i = x+(f)$, $f = x^2+1$

Definiere $\iota: \mathbb{R} \to \mathbb{C}$, $a \mapsto a+(f)$. Dann gilt $\mathbb{C} =$
$\{a+bx+(f) \mid a,b \in \mathbb{R}\} = \{\iota(a)+\iota(b)\cdot i \mid a,b \in \mathbb{R}\}$ und
$$i^2 = (x+(f))^2 = x^2+(f) = -1+(f) = -1_{\mathbb{C}}$$
$$x^2-(-1) = x^2+1 \in (f)$$

Restklassenringe als Körper

Der folgende Satz ist bereits aus der Linearen Algebra bekannt.

Satz (11.7)

Sei $n \in \mathbb{N}$. Genau dann ist $\mathbb{Z}/n\mathbb{Z}$ ein Körper, wenn n eine Primzahl ist.

Der induzierte Homomorphismus

Proposition (11.8)

Sei $\phi : R \to R'$ ein Ringhomomorphismus und $I \subseteq R$ ein Ideal mit $I \subseteq \ker(\phi)$. Dann gibt es einen eindeutig bestimmten Homomorphismus

$$\bar{\phi} : R/I \longrightarrow R' \qquad \text{mit} \quad \bar{\phi}(a+I) = \phi(a) \quad \text{für alle} \quad a \in R.$$

Man bezeichnet ihn als den von ϕ induzierten Homomorphismus.

Beweis von Proposition 11.8

z.zg. Es gibt einen Hom. $\bar{\Phi} : R/I \to R'$ mit $\bar{\Phi}(a+I) = \phi(a) \ \forall a \in R$, unter der Voraussetzung, das der Ringhom. $\phi : R \to R'$ die Bedingung $I \subseteq \ker(\phi)$ erfüllt.

Nach Satz 4.25 genügt es zu zeigen, dass für alle $a, a' \in R$ mit $a \equiv a' \bmod I$ jeweils $\phi(a) = \phi(a')$ gilt. Seien also a, a' mit dieser Eigenschaft vorgeg. $a \equiv a' \bmod I \Rightarrow$
$a' - a \in I \Rightarrow a' - a \in \ker(\phi) \Rightarrow \phi(a) =$
$\phi(a) + 0_{R'} = \phi(a) + \phi(a'-a) = \phi(a + (a'-a)) = \phi(a')$.

überprüfe: $\bar{\Phi}$ ist ein Ringhomomorphismus

Zunächst gilt $\bar{\Phi}(1_{R/I}) = \bar{\Phi}(1_R + I) = \phi(1_R) = 1_{R'}$. Für alle $a, b \in R$ gilt außerdem

$$\bar{\Phi}((a+I)+(b+I)) = \bar{\Phi}((a+b)+I) = \phi(a+b) = \phi(a)+\phi(b) = \bar{\Phi}(a+I)+\bar{\Phi}(b+I),$$

ebenso

$$\bar{\Phi}((a+I)\cdot(b+I)) = \bar{\Phi}(ab+I) = \phi(ab) = \phi(a)\phi(b) = \bar{\Phi}(a+I)\cdot\phi(b+I).$$

$\square$

Der Homomorphiesatz für Ringe

Satz (11.9)

Sei $\phi : R \to R'$ ein Homomorphismus von Ringen und $I = \ker(\phi)$. Dann induziert ϕ einen Isomorphismus

$$\bar{\phi} : R/I \xrightarrow{\sim} \operatorname{im}(\phi)$$

von Ringen.

Beweis des Homomorphiesatzes:

Sei $\phi : R \to R'$ ein Ringhom., $I = \ker(\phi)$
und $\bar{\phi} : R/I \to R'$ der induzierte Homomorphismus. Für alle $a \in R$ gilt $\bar{\phi}(a+I) =$
$\phi(a) \in \mathrm{im}(\phi) \Rightarrow$ können $\bar{\phi}$ als Abbildung
$R/I \to \mathrm{im}(\phi)$ auffassen. Nach Prop. 11.8 ist
dies ein Ringhom.

Surjektivität: Sei $c \in \mathrm{im}(\phi) \Rightarrow \exists\, a \in R$ mit

$$\phi(a) = c \Rightarrow \bar{\phi}(a+I) = c.$$

Injektivität: Überprüfe $\ker(\bar{\phi}) \subseteq \{0_{R/I}\}$

Sei $a+I \in \ker(\bar{\phi})$, mit $a \in I \to \bar{\phi}(a+I) =$
$0_{R'} \Rightarrow \phi(a) = 0_{R'} \Rightarrow a \in \ker(\phi)$

Korrektur vorletzte Zeile: „Sei $a + I \in \ker(\bar{\phi})$, mit $a \in R$.“

$$\Rightarrow a \in I \Rightarrow a + I = I = 0_R + I = 0_{R/I}$$

$$\Rightarrow a + I \in \{0_{R/I}\} \qquad \square$$

)

g
ist

mit

$I) =$