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.

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

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

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

Nebenklassen in Polyomringen

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

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

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

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 $a, b \in R$.

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.

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.

Weiteres Beispiel für einen Faktorring

$R = \mathbb{R}[x]$, $f = x^2 + 1$, $I = (f)$

$\mathbb{C} = \mathbb{R}[x]/I = \{a + bx + I \mid a, b \in \mathbb{R}\}$

↑ Aufg. 11.4

Sei $i = x + I$. Dann $i^2 = (x + I)^2 = (x + I)(x + I)$

$= x^2 + I = x^2 + (-1)\cdot(x^2 + 1) + I = -1 + I = -1_{\mathbb{C}}$

↑ $(-1)\cdot(x^2 + 1) \in I$

Sei $\phi : \mathbb{R} \to \mathbb{R}[x]/I$, $a \mapsto a + I$. Dann gilt

jeweils $a + bx + I = (a + I) + (b + I)\cdot(x + I)$

$= \phi(a) + \phi(b) \cdot i \quad \forall a, b \in \mathbb{R}$

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 Prop. 11.8

geg.: Ringhom. $\phi: R \to R'$, $I \subseteq R$ Ideal mit $I \subseteq \ker(\phi)$

z.zg.: $\exists$ Ringhom $\bar{\phi}: R/I \to R'$ mit $\bar{\phi}(a+I) = \phi(a)$ $\forall a \in R$

Wende Satz 4.25 (i) an auf die Abb. ϕ und die Kongruenzrelation modulo I, zu überprüfen. Für alle $a, b \in R$ mit $a \equiv b \bmod I$ gilt $\phi(a) = \phi(b)$. Seien also a, b mit dieser Eig. vorgeg. $a \equiv b \bmod I \Rightarrow b - a \in I \overset{\text{Vor.}}{\Rightarrow}$

$b - a \in \ker(\phi) \Rightarrow \phi(b) = \phi(b - a + a) = \phi(b-a) + \phi(a)$

$= 0_{R'} + \phi(a) = \phi(a)$. Also existiert eine Abbildung $\bar{\phi}: R/I$ mit der angeg. Eigenschaft. □

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

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

von Ringen.

Beweis des Homomorphiesatzes

Sei $\bar{\phi} : R/I \to R'$ der durch ϕ induzierte Homomorphismus. Für alle $a + I \in R/I$ (mit $a \in R$) gilt $\bar{\phi}(a + I) = \phi(a) \in \mathrm{im}(\phi)$. Somit kann $\bar{\phi}$ als Abbildung $R/I \to R'$ aufgefasst werden. Diese Abbildung ist surjektiv. Denn für jedes $c \in \mathrm{im}(\phi)$ existiert ein $a \in R$ mit $\phi(a) = c$, und es folgt $\bar{\phi}(a + I) = \phi(a) = c$.

Für den Nachweis der Injektivität genügt es, $\ker(\bar{\phi}) \subseteq \{0_{R/I}\}$ zu überprüfen. Sei also $a + I \in \ker(\bar{\phi})$, mit $a \in R$. Dann gilt $\bar{\phi}(a + I) = 0_{R'}$, und es folgt $\phi(a) = 0_{R'}$. Somit ist a ein Element von $I = \ker(\phi)$, und es folgt $a + I = I = 0_{R/I}$.

Korrespondenzsatz für Ideale

Satz (11.10)

Sei R ein Ring, I ein Ideal und $\pi : R \to R/I$ der kanonische Epimorphismus. Sei $\bar{\mathcal{I}}$ die Menge der Ideale von R/I und $\mathcal{I}_I$ die Menge der Ideale J von R mit $J \supseteq I$.

(i) Die Zuordnungen $\phi : \mathcal{I}_I \to \bar{\mathcal{I}}$, $J \mapsto \pi(J)$ und $\psi : \bar{\mathcal{I}} \to \mathcal{I}_I$, $\bar{J} \mapsto \pi^{-1}(J)$ sind bijektiv und zueinander invers.

(ii) Für alle Ideale $J, K \in \mathcal{I}_I$ gilt $J \subseteq K \Leftrightarrow \pi(J) \subseteq \pi(K)$.

Körper als Faktorringe

Lemma (11.11)

Ein Ring ist genau dann ein Körper, wenn (0) und (1) die einzigen Ideale des Rings sind und $(0) \neq (1)$ gilt.

Satz (11.12)

Sei R ein Ring, $\mathfrak{p} \subseteq R$ ein Ideal und $\bar{R} = R/\mathfrak{p}$.

(i) Genau dann ist $\mathfrak{p}$ ein Primideal, wenn $\bar{R}$ ein Integritätsbereich ist.

(ii) Genau dann ist $\mathfrak{p}$ ein maximales Ideal, wenn $\bar{R}$ ein Körper ist.

Folgerung (11.13)

Jedes maximale Ideal ist ein Primideal.

Beweis von Lemma 11.11

Sei R ein Ring. Zu zeigen ist, dass R genau dann ein Körper ist, wenn R genau zwei Ideale besitzt, nämlich (0_R) und (1_R).

„$\Rightarrow$“ Sei I ein Ideal in R, und nehmen wir an, es ist $I \neq (0_R)$. Dann gibt es ein $a \in I \setminus \{0_R\}$. Weil R ein Körper ist, existiert der Kehrwert a^{-1} in R. Aus $a^{-1} \in R$ und $a \in I$ folgt $1_R = a^{-1} \cdot a \in I$ und damit $(1_R) \subseteq I$. Wegen $(1_R) = R$ erhalten wir $I = (1_R)$. Es gibt also außer (0_R) und (1_R) keine Ideale in R.

Nehmen wir nun an, dass $(1_R) = (0_R)$ ist. Dann folgt $1_R \in \{0_R\}$ und $1_R = 0_R$. Aber in einem Integritätsbereich stimmen 1_R und 0_R nicht überein, und erst recht ist das in einem Körper nicht möglich.

„$\Leftarrow$" z.zg für die Körpereigenschaft:

$R^\times = R \setminus \{0_R\}$ „$\subseteq$" Ang. „$\subseteq$" gilt nicht.

$\Rightarrow 0_R$ ist Einheit $\Rightarrow \exists\, c \in R$ mit $0_R \cdot c = 1_R$

$\Rightarrow 0_R = 0_R \cdot c = 1_R \Rightarrow (0_R) = (1_R)$ ↯

„$\supseteq$" Sei $a \in R \setminus \{0_R\}$, z.zg.: $a \in R^\times$

Sei $I = (a)$ $a \neq 0_R \Rightarrow I \neq (0_R) \Rightarrow I = (1_R)$

$\Rightarrow 1_R \in (a) \Rightarrow \exists\, c \in R$ mit $ca = 1_R$

$\Rightarrow a \in R^\times$. □

Beweis von Satz 11.12

geg.: R Ring, $\mathfrak{p}$ Ideal von R, $\bar{R} = R/\mathfrak{p}$

zu ii) Beh.: $\mathfrak{p}$ ist Primideal $\Leftrightarrow$ $\bar{R}$ Integritätsbereich

„$\Rightarrow$" Vor.: $\mathfrak{p}$ ist Primideal, z.zg.: $0_{\bar{R}}$ ist der einzige Nullteiler von $\bar{R}$

(1) $0_{\bar{R}}$ ist Nullteiler, denn: $\mathfrak{p}$ Primideal $\Rightarrow$ $\mathfrak{p} \neq (1_R) \Rightarrow 1_R \notin \mathfrak{p} \Rightarrow 1_R + \mathfrak{p} \neq \mathfrak{p} \Rightarrow$ $1_{\bar{R}} \neq 0_{\bar{R}} \Rightarrow 0_{\bar{R}}$ ist Nullteiler (wg. $0_{\bar{R}} \cdot 1_{\bar{R}} = 0_{\bar{R}}$, $1_R \neq 0_R$)

(2) Es gibt keinen Nullteiler ungleich $0_{\bar{R}}$, denn: Ang. $a + \mathfrak{p}$ ist Nullteiler $\neq 0_{\bar{R}}$, mit $a \in R$.

$\Rightarrow \exists\, b+\mathfrak{p} \in \bar{R} \setminus \{0_{\bar{R}}\}$ mit $b \in R$ und $(a+\mathfrak{p})\cdot(b+\mathfrak{p})$

$= 0_{\bar{R}}$ $\quad a+\mathfrak{p},\ b+\mathfrak{p} \neq 0_{\bar{R}} \Rightarrow a, b \notin \mathfrak{p}$

$(a+\mathfrak{p})\cdot(b+\mathfrak{p}) = 0_{\bar{R}} = \mathfrak{p} \Rightarrow ab+\mathfrak{p} = \mathfrak{p} \Rightarrow ab \in \mathfrak{p}$

also: $ab \in \mathfrak{p},\ a \notin \mathfrak{p},\ b \notin \mathfrak{p}$ $\lightning$ zu Primideal-Eig. von $\mathfrak{p}$

Beweis von Satz 11.12 (Forts.)

R Ring, $\mathfrak{p}$ Ideal, $\bar{R} = R/\mathfrak{p}$

noch z.zg.: $\bar{R}$ Integritätsbereich $\Rightarrow$ $\mathfrak{p}$ ist Primideal

zu überprüfen (1) $\mathfrak{p} \neq (1_R)$

(2) $\forall a, b \in R: ab \in \mathfrak{p} \Rightarrow a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$

zu (1) Ang. $\mathfrak{p} = (1_R) \rightarrow 1_R \in \mathfrak{p} \Rightarrow 1_R + \mathfrak{p} = \mathfrak{p} \Rightarrow$

$1_{\bar{R}} = 0_{\bar{R}}$ ↯ zu $\bar{R}$ Integritätsbereich

zu (2) Seien $a, b \in R$ mit $ab \in \mathfrak{p}$ z.zg.: $a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$

$ab \in \mathfrak{p} \Rightarrow ab + \mathfrak{p} = \mathfrak{p} \Rightarrow (a+\mathfrak{p})(b+\mathfrak{p}) = 0_{\bar{R}}$

$\bar{R}$ ist Integritätsbereich $\Rightarrow$ $a + \mathfrak{p} = 0_{\bar{R}}$ oder $b + \mathfrak{p} = 0_R \Rightarrow$

$a + \mathfrak{p} = \mathfrak{p}$ oder $b + \mathfrak{p} = \mathfrak{p} \Rightarrow a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$

zu ii) Beh.: $\mathfrak{p}$ ist maximal $\Longleftrightarrow$ $\overline{R}$ ist Körper

$\mathfrak{p}$ ist maximal $\Longleftrightarrow$ $\mathfrak{p} \subsetneq (1_R)$ und es gibt kein Ideal J mit $\mathfrak{p} \subsetneq J \subsetneq (1_R)$ $\Longleftrightarrow$ Es gibt genau zwei Ideale I mit $I \supseteq \mathfrak{p}$: nämlich $\mathfrak{p}$ und (1_R)

Korrespondenz-Satz $\Longrightarrow$ Der Ring $\overline{R}$ besitzt genau zwei Ideale: die Bilder von $\mathfrak{p}$ und (1_R) in $\overline{R}$ (Dies sind das Nullideal $(0_{\overline{R}})$ und das Einsideal $(1_{\overline{R}})$ in $\overline{R}$.)

Lemma 11.11 $\Longleftrightarrow$ $\overline{R}$ ist Körper

□

Übertragung von Verknüpfungen

Lemma (11.14)

Seien X und Y Mengen, $\phi : Y \to X$ eine Bijektion und $\cdot$ eine Verknüpfung auf X. Wir definieren auf Y eine Vernüpfung $\odot$, indem wir $a \odot b = \phi^{-1}(\phi(a) \cdot \phi(b))$ für alle $a, b \in Y$ definieren. Die neue Verknüpfung $\odot$ hängt dann mit $\cdot$ auf folgende Weise zusammen.

(i) Ist die Verknüpfung $\cdot$ auf X assoziativ bzw. kommutativ, dann gilt dasselbe jeweils für die Verknüpfung $\odot$ auf Y.

(ii) Ist $e_X \in X$ ein Neutralelement in X bezüglich $\cdot$, dann ist $e_Y = \phi^{-1}(e_X)$ ein Neutralelement in Y bezüglich $\odot$.

(iii) Seien e_X und e_Y wie in (ii) und $a, b \in X$. Ist b ein Inverses von a bezüglich $\cdot$, dann ist $\phi^{-1}(b)$ ein Inverses von $\phi^{-1}(a)$ bezüglich $\odot$.

zum Beweis von Lemma 11.14:

geg.: Verknüpfung $\cdot$ auf einer Menge X

$\phi : Y \to X$ Bijektion

Verknüpfung $\odot$ auf Y geg. durch $a \odot b = \phi^{-1}(\phi(a) \cdot \phi(b))$

$\forall a, b \in Y \; (\to \phi(a \odot b) = \phi(a) \cdot \phi(b) \quad \forall a, b \in Y)$

zeige: Erfüllt $\cdot$ das Assoziativgesetz, dann auch $\odot$

Seien $a, b, c \in Y$. $\phi((a \odot b) \odot c) = \phi(a \odot b) \cdot \phi(c)$

$= (\phi(a) \cdot \phi(b)) \cdot \phi(c) = \phi(a) \cdot (\phi(b) \cdot \phi(c)) =$

[Ass.-gesetz in X

$\phi(a) \cdot \phi(b \odot c) = \phi(a \odot (b \odot c)) \overset{\phi^{-1}}{\Rightarrow} (a \odot b) \odot c = a \odot (b \odot c)$ □

Übertragung einer Ringstruktur

Satz (11.15)

Sei $(R, +, \cdot)$ ein Ring, S eine Menge und $\phi : S \to R$ eine bijektive Abbildung. Seien die Verknüpfungen $\oplus$ und $\odot$ auf S definiert durch

$$a \oplus b = \phi^{-1}(\phi(a) + \phi(b)) \qquad \text{und} \qquad a \odot b = \phi^{-1}(\phi(a) \cdot \phi(b)).$$

Dann ist $(S, \oplus, \odot)$ ein Ring, und ϕ ist ein Isomorphismus von Ringen.

Konstruktion von Ringerweiterungen

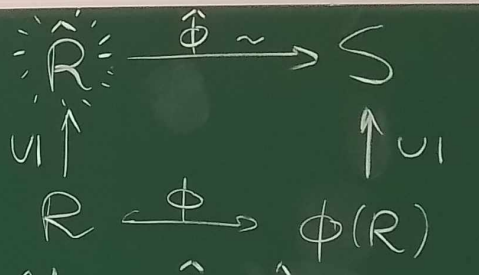
Satz (11.16)

Sei $\phi : R \to S$ ein Monomorphismus von Ringen. Dann gibt es einen Erweiterungsring $\hat{R} \supseteq R$ und einen Isomorphismus $\hat{\phi} : \hat{R} \to S$ mit $\hat{\phi}|_R = \phi$.

Anwendung:

Konstruktion des Körpers $\mathbb{C}$ der komplexen Zahlen

Beweis von Satz 11.16



Definiere $\hat{R} = (S \setminus \phi(R)) \cup R$.

Dann gilt $R \subseteq \hat{R}$. Definiere nun eine Abbildung $\hat{\phi}: \hat{R} \to S$

durch $\hat{\phi}(a) = \begin{cases} \phi(a) & \text{falls } a \in R \\ a & \text{sonst} \end{cases}$ überprüfe: $\hat{\phi}$ ist bijektiv

Verwende diese Bijektion, um gemäß Lemma 11.14 Verknüpfungen $\oplus$ und $\odot$ auf $\hat{R}$ zu definieren. Nach Satz 11.15 ist $\hat{R}$ dann ein Ring. Für alle $a, b \in R$ gilt $\hat{\phi}(a \oplus b) = \hat{\phi}(a) + \hat{\phi}(b) = \phi(a) + \phi(b) = \phi(a+b) = \hat{\phi}(a+b) \overset{\hat{\phi}^{-1}}{\Rightarrow}$

$\Sigma_{a,b \in R}$ $\Sigma_{a+b \in R}$

$\Rightarrow a \oplus b = a + b$. Ebenso überprüft man, dass $a \odot b =$

$a \cdot b$ für alle $a, b \in R$ gilt. Es ist nun leicht zu sehen, dass R ein Teilring von $\hat{R}$ ist, denn: $1_{\hat{R}} = 1_R$, da $a \odot 1_R = a$ für alle $a \in S$ gilt (sowohl im Fall $a \in R$ als auch im Fall $a \in S \setminus \phi(R)$ $\overset{(*)}{\Rightarrow} 1_{\hat{R}} \in R$

Ebenso gilt $0_{\hat{R}} = 0_R$, und für jedes $a \in R$ ist $-a$ das Negative von a in $(\hat{R}, \oplus, \odot)$, da $a \oplus (-a) = a + (-a) = 0_R = 0_{\hat{R}}$ $\Rightarrow$ Für alle $a, b \in R$ gilt somit $a \ominus b = a - b \in R$ (wobei $\ominus b$ Negatives von b in $(\hat{R}, \oplus, \odot)$, und ebenso $a \odot b = ab \in R$ ($\rightarrow$ Teilring-Eig.)

Schließlich ist $\hat{\phi} : \hat{R} \to S$ ein Ringisom., denn $\hat{\phi}(1_{\hat{R}}) = \hat{\phi}(1_R) = \phi(1_R) = 1_S$, und für alle $a, b \in \hat{R}$ gilt $\hat{\phi}(a \oplus b) = \hat{\phi}(a) + \hat{\phi}(b)$, $\hat{\phi}(a \odot b) = \hat{\phi}(a) \cdot \hat{\phi}(b)$, nach Def. von $\oplus$ und $\odot$, und $\hat{\phi}$ ist bij.

(*) 1. Fall: $a \in R$ $\quad \hat{\phi}(a \odot 1_R) = \hat{\phi}(a)\,\hat{\phi}(1_R) =$

$\phi(a) \cdot \phi(1_R) = \phi(a \cdot 1_R) = \phi(a) = \hat{\phi}(a) \overset{\hat{\phi}^{-1}}{\Rightarrow}$

$a \odot 1_R = a$

2. Fall: $a \in S \setminus \phi(R)$ $\quad \hat{\phi}(a \odot 1_R) = \hat{\phi}(a)\,\hat{\phi}(1_R)$

$= a \cdot 1_R = a = \hat{\phi}(a) \overset{\hat{\phi}^{-1}}{\Rightarrow} a \odot 1_R = a$ $\quad \square$