10. MODULORECHNEN

In diesem Kapitel sind Ringe immer kommutative Ringe mit 1. Erinnerung: Ein kommutativer Ring mit 1 ist ein Modell der Ringaxiome $\mathsf{RT}_0 - \mathsf{RT}_8$, also eine $\mathscr{L}_{\mathsf{RT}}$-Struktur mit Bereich R, wobei $\mathscr{L}_{\mathsf{RT}} = \{0, 1, +, \cdot\}$. Wie üblich identifizieren wir einen Ring $(R, 0, 1, +, \cdot)$ mit seinem Bereich R, oder wir schreiben $(R, +, \cdot)$ um auch die binären Operationen hervorzuheben.

IDEALE

Sei $(R, 0, 1, +, \cdot)$ ein kommutativer Ring. Eine Menge $I \subseteq R$ ist ein **Ideal** in R, falls die folgenden Bedingungen erfüllt sind:

(I_0) $I \neq \emptyset$
(I_1) $\forall a, b \in I\,(a + b \in I)$
(I_2) $\forall x \in R \forall a \in I\,(x \cdot a \in I)$

Da mit $1 \in R$ auch $-1 \in R$ ist, folgt aus (I_2), dass mit jedem $a \in I$ auch $(-1) \cdot a = -a$ in I ist. Mit (I_0) und (I_1) ist das Ideal also eine additive Untergruppe von R, d. h. eine Untergruppe der abelschen Gruppe $(R, 0, +)$. Ist $1 \in I$, so ist $I = R$ (also ein Ring), ist aber $1 \notin I$ und $I \neq \{0\}$, so ist I kein Unterring von R (nicht-triviale Unterringe von R müssen die 1 enthalten). Beachte, dass $\{0\}$ ein Ring mit 1 ist – in $\{0\}$ gilt $0 = 1$.

Jeder Ring R besitzt die beiden *trivialen* Ideale R und $\{0\}$; das Ideal $\{0\}$ heisst **Nullideal**. Wie wir später sehen werden, sind Körper dadurch charakterisiert, dass sie nur die trivialen Ideale enthalten.

Beispiele: (a) Für $m \in \mathbb{Z}$ sei

$$m\mathbb{Z} := \{x \cdot m : x \in \mathbb{Z}\}.$$

Dann ist $m\mathbb{Z}$ ein Ideal im Ring $(\mathbb{Z}, 0, 1, +, \cdot)$. Denn mit $xm \in m\mathbb{Z}$ ist auch $y \cdot (xm) = (yx) \cdot m \in I$, und mit $xm, ym \in I$ ist auch $xm + ym = (x + y)m \in I$.

(b) Sei $\mathbb{Z}[X]$ der Ring der Polynome mit Koeffizienten in $\mathbb{Z}$ (siehe Aufgabe 11), und sei $f \in \mathbb{Z}[X]$, zum Beispiel $f = 1 - X^2 + 7X^3$. Dann ist

$$(f) := \big\{g \cdot f : g \in \mathbb{Z}[X]\big\}$$

ein Ideal in $\mathbb{Z}[X]$: Nach Definition sind (I_0) und (I_2) erfüllt, und weil $\mathbb{Z} \subseteq \mathbb{Z}[X]$, ist mit ($\mathrm{I}_2$) auch ($\mathrm{I}_1$) erfüllt.

Für Beispiel (a) gilt auch eine Art Umkehrung.

PROPOSITION 10.1. *Ist $I \subseteq \mathbb{Z}$ ein Ideal, dann existiert ein $m \in \mathbb{Z}$, sodass gilt:*

$$I = m\mathbb{Z}$$

Beweis. Ist I das Nullideal, so ist $I = 0\mathbb{Z}$ und wir sind fertig. Ist $I \neq \{0\}$, so enthält I mit (I_2) positive Zahlen. Sei

$$m := \min\big\{n \in \mathbb{N} \setminus \{0\} : n \in I\big\}.$$

Wir zeigen $I = m\mathbb{Z}$. Für einen Widerspruch nehmen wir an, dass ein $a \in I$ existiert mit $a \notin m\mathbb{Z}$. Wir dürfen annehmen, dass $a > 0$, denn mit $a \in I$ ist immer auch $-a \in I$. Nach Definition von m ist $m < a$. Sei $d := \mathrm{ggT}(a, m)$. Dann ist $1 \leq d < m$, weil $a \notin m\mathbb{Z}$. Mit dem vEA finden wir $k, l \in \mathbb{Z}$ mit $ka + lm = d$. Aus (I_2) folgt, dass sowohl ka wie auch lm in I sind, und mit (I_1) ist somit auch $ka + lm$, also $d < m$ in I, was aber der Definition von m widerspricht. ⊣

FAKTORRINGE

Sei R ein kommutativer Ring und sei $I \subseteq R$ ein Ideal, zum Beispiel $R = \mathbb{Z}$ und $I = m\mathbb{Z}$ für ein $m \in \mathbb{Z}$. Für $x \in R$ definieren wir die sogenannte **Restklasse** von x durch

$$\bar{x} := x + I = \{x + a : a \in I\}.$$

Weiter definieren wir auf R die binäre Relation "$\sim$" durch:

$$x \sim y \iff \bar{x} = \bar{y}$$

Weil "$=$" eine Äquivalenzrelation ist, ist auch "$\sim$" eine Äquivalenzrelation. Gilt $x \sim y$, so sagen wir "x ist kongruent y modulo I" und schreiben

$$x \equiv y \pmod{I}.$$

Sei $R/I := \{\bar{x} : x \in R\}$ (gesprochen "R *modulo* I") die Menge der Äquivalenzklassen. Auf R/I definieren wir die beiden binären Operationen $\oplus$ und $\otimes$ auf Repräsentanten von Äquivalenzklassen wie folgt:

$$\bar{x} \oplus \bar{y} := \overline{x + y} \qquad \text{und} \qquad \bar{x} \otimes \bar{y} := \overline{x \cdot y}$$

Das folgenden Lemma zeigt, dass die Operationen $\oplus$ und $\otimes$ wohldefiniert (d. h. unabhängig von der Wahl der Repräsentanten) sind.

LEMMA 10.2. *Seien $x_0, x_1, y_0, y_1 \in R$, sodass gilt $\bar{x}_0 = \bar{x}_1$ und $\bar{y}_0 = \bar{y}_1$. Dann gilt:*

$$\bar{x}_0 \oplus \bar{y}_0 = \bar{x}_1 \oplus \bar{y}_1 \qquad \textit{und} \qquad \bar{x}_0 \otimes \bar{y}_0 = \bar{x}_1 \otimes \bar{y}_1$$

Beweis. Beachte, dass für alle $x, y \in R$ gilt:

$$x \in I \Rightarrow (x + I) = I \qquad \text{und} \qquad x + I = y + I \iff x - y \in I$$

$\oplus$ ist wohldefiniert: Seien nun $x_0, x_1, y_0, y_1 \in R$, sodass gilt $\bar{x}_0 = \bar{x}_1$ und $\bar{y}_0 = \bar{y}_1$. Es gilt nun:

$$\begin{aligned}\overline{x_0 + y_0} = (x_0 + y_0) + I = (x_0 + I) + (y_0 + I) = \\ \big(x_0 + \big(\underbrace{(x_1 - x_0)}_{\in I} + I\big)\big) + \big(y_0 + \big(\underbrace{(y_1 - y_0)}_{\in I} + I\big)\big) = \\ (x_1 + I) + (y_1 + I) = (x_1 + y_1) + I = \overline{x_1 + y_1}\end{aligned}$$

Somit ist $\overline{x_0 + y_0} = \overline{x_1 + y_1}$, d. h. $\bar{x}_0 \oplus \bar{y}_0 = \bar{x}_1 \oplus \bar{y}_1$.

$\otimes$ ist wohldefiniert: Weil nach Voraussetzung $\bar{x}_0 = \bar{x}_1$ und $\bar{y}_0 = \bar{y}_1$, gilt $x_0 - x_1 \in I$ und $y_0 - y_1 \in I$. Somit haben wir

$$\left.\begin{aligned} x_0 \cdot (y_0 - y_1) = \quad x_0 y_0 - x_0 y_1 \in I \\ y_1 \cdot (x_0 - x_1) = -x_1 y_1 + x_0 y_1 \in I \end{aligned}\right\} \Rightarrow (x_0 y_0 - x_1 y_1) \in I,$$

woraus folgt $x_0 y_0 + I = x_1 y_1 + I$, d. h. $\overline{x_0 \cdot y_0} = \overline{x_1 \cdot y_1}$. Somit ist $\bar{x}_0 \otimes \bar{y}_0 = \bar{x}_1 \otimes \bar{y}_1$. ⊣

Mit Lemma 10.2 können wir die Ringstruktur vom Ring R auf R/I übertragen und erhalten, dass $\big(R/I, \bar{0}, \bar{1}, \oplus, \otimes\big)$ ein kommutativer Ring ist (den Beweis lassen wir weg). Der Ring R/I ist ein sogenannter **Faktorring**.

DIE RINGE $\mathbb{Z}_m$

In diesem Abschnitt betrachten wir den Faktorring $\mathbb{Z}/I$, wobei $I \subseteq \mathbb{Z}$ ein Ideal ist, d. h. $I = m\mathbb{Z}$ für ein $m \in \mathbb{Z}$. Die Elemente von $\mathbb{Z}/I$ bezeichnen wir wieder mit $\bar{x}, \bar{y}, \ldots$, aber anstelle von "$\oplus$" und "$\otimes$" schreiben wir "$+$" bzw. "$\cdot$", wobei wir den Multiplikationspunkt wie üblich auch manchmal weglassen. Da Ideale $I \subseteq \mathbb{Z}$ immer von der Form $I = m\mathbb{Z}$ sind für ein $m \in \mathbb{Z}$, schreiben wir $\mathbb{Z}_m$ anstelle von $\mathbb{Z}/m\mathbb{Z}$.

Für $m \geq 1$ ist somit $\mathbb{Z}_m$ ein Ring mit den m Elementen $\bar{0}, \ldots, \overline{m-1}$, insbesondere ist $\mathbb{Z}_1 = \mathbb{Z}/\mathbb{Z}$ der Nullring $\{\bar{0}\}$. Weiter ist die Struktur $(\mathbb{Z}_m, \bar{0}, +)$ eine Gruppe welche durch $\bar{1}$ erzeugt wird, d. h. jedes Element $a \in \mathbb{Z}_m$ ist von der Form $a = \bar{1} + \ldots + \bar{1}$. Andererseits ist für $m \geq 2$, $(\mathbb{Z}_m \setminus \{\bar{0}\}, \bar{1}, \cdot)$ im Allgemeinen keine Gruppe (z. B. hat $\bar{6}$ in $\mathbb{Z}_{15}$ kein multiplikativ Inverses). Mit der folgenden Proposition lassen sich die Elemente von $\mathbb{Z}_m$ bestimmen, welche ein multiplikativ Inverses haben.

PROPOSITION 10.3. *Sei $m \geq 2$ und sei $\bar{a} \in \mathbb{Z}_m$. Dann existiert genau dann ein $\bar{b} \in \mathbb{Z}_m$ mit $\bar{a} \cdot \bar{b} = \bar{1}$, wenn $\mathrm{ggT}(a, m) = 1$.*

Beweis. Sei $d := \mathrm{ggT}(a, m)$. Existiert ein $\bar{b} \in \mathbb{Z}_m$ mit $\bar{a} \cdot \bar{b} = \bar{1}$, so erhalten wir $ab = ml + 1$ für ein $l \in \mathbb{Z}$. Aus $d \mid a$ und $d \mid m$ folgt dann $d \mid (ab - ml)$, d. h. $d \mid 1$. Somit muss $d = 1$ sein.

Ist nun $\mathrm{ggT}(a, m) = 1$, so finden wir mit dem vEA Zahlen $b, l \in \mathbb{Z}$ mit $ab + ml = 1$. Das heisst $ab \equiv 1 \pmod{m}$, woraus folgt $\overline{ab} = \bar{a} \cdot \bar{b} = \bar{1}$. ⊣

Wenn wir nur die Elemente aus $\mathbb{Z}_m \setminus \{\bar{0}\}$ betrachten, welche ein multiplikativ Inverses haben, so bilden diese Elemente bezüglich der Multiplikation eine Gruppe, die sogenannte **Einheitengruppe** des Rings $\mathbb{Z}_m$, welche wir mit $\mathbb{Z}_m^*$ bezeichnen. Um zu sehen, dass $\mathbb{Z}_m^*$ eine multiplikative Gruppe ist, genügt es zu zeigen, dass mit $\bar{a}, \bar{b} \in \mathbb{Z}_m^*$ auch $\bar{a}\bar{b}$ in $\mathbb{Z}_m^*$ ist. Das folgt aber direkt aus den Eigenschaften des ggT, denn wenn $\mathrm{ggT}(a, m) = 1$ und $\mathrm{ggT}(b, m) = 1$, dann ist auch $\mathrm{ggT}(ab, m) = 1$. Die Ordnung der Gruppe $\mathbb{Z}_m^*$ wird mit $\varphi(m)$ bezeichnet, also $\varphi(m) := |\mathbb{Z}_m^*|$ und φ heisst **Euler'sche φ-Funktion**. Es gilt der folgende Satz (den wir nicht beweisen):

EULER'SCHER SATZ. *Für $m \geq 2$ und $\mathrm{ggT}(a, m) = 1$ gilt:*

$$a^{\varphi(m)} \equiv 1 \pmod{m} \quad \textit{bzw.} \quad m \mid a^{\varphi(m)} - 1$$

Als Spezialfall des Euler'schen Satzes erhalten wir für Primzahlen m den folgenden Satz (beachte, dass für Primzahlen m gilt $\varphi(m) = m - 1$):

KLEINER SATZ VON FERMAT. *Für p prim und $\mathrm{ggT}(a, p) = 1$ gilt:*

$$a^{p-1} \equiv 1 \pmod{p} \quad \textit{bzw.} \quad p \mid a^p - a$$

Beweis. Sei p prim und $\mathrm{ggT}(a, p) = 1$. Wir betrachten die Punkte eines regelmässigen p-Ecks, welche wir mit a verschiedenen Farben färben. Es existieren a^p verschiedene Färbungen, wobei es neben den a einfarbigen Färbungen $a^p - a$ Färbungen gibt, welche mindestens zwei Farben haben. Da p prim ist, kann keine Färbung, die mindestens zwei Farben hat, durch eine Drehung um $k\frac{2\pi}{p}$ mit $k \in \{1, \ldots, p-1\}$ in sich übergeführt werden. Zwei Färbungen, die mindestens zwei Farben haben, seien äquivalent, wenn sie durch eine Drehung um $k\frac{2\pi}{p}$ für ein $k \in \{0, \ldots, p-1\}$ ineinander übergeführt werden können. Dann hat jede Äquivalenzklasse genau p Element und somit lässt sich $a^p - a$ durch p teilen. ⊣

DIE KÖRPER $\mathbb{F}_p$

Für $m \geq 2$ ist der Ring $(\mathbb{Z}_m, \bar{0}, \bar{1}, +, \cdot)$ genau dann ein Körper, wenn jedes Element aus $\mathbb{Z}_m \setminus \{\bar{0}\}$ ein multiplikativ Inverses besitzt. Mit Proposition 10.3 ist dies genau dann der Fall, wenn für jedes $\bar{a} \in \mathbb{Z}_m \setminus \{\bar{0}\}$ gilt $\mathrm{ggT}(a, m) = 1$. Das ist genau dann erfüllt, wenn m eine Primzahl ist: Denn ist m eine Primzahl und $1 \leq a < m$, so ist $\mathrm{ggT}(a, m) = 1$. Ist andererseits m keine Primzahl, so existiert ein $1 < a < m$ mit $a \mid m$. Das heisst $\bar{a} \in \mathbb{Z}_m \setminus \{\bar{0}\}$, $\mathrm{ggT}(a, m) > 1$ und $\bar{a}$ hat kein multiplikativ Inverses.

Der Ring $\mathbb{Z}_m$ ist also genau dann ein Körper (engl. *field*), wenn m eine Primzahl ist. Die Körper $\mathbb{Z}_p$ für p prim werden mit $\mathbb{F}_p$ bezeichnet.

Etwas allgemeiner erhalten wir für Ringe R, dass R/I genau dann ein Körper ist, wenn das Ideal I maximal ist, wobei ein Ideal I ein **maximales Ideal** ist, wenn $I \neq R$ und I in keinem echten Ideal $J \subsetneq R$ echt enthalten ist.

PROPOSITION 10.4. *Sei R ein Ring und sei $I \neq R$ ein Ideal von R. Dann ist R/I genau dann ein Körper, wenn I ein maximales Ideal ist.*

Beweis. ($\Leftarrow$): Wir zeigen diese Richtung mit Kontraposition. Sei $I \subsetneq R$ ein Ideal und sei R/I kein Körper. Dann existiert ein $a_0 \in R \setminus I$ (d. h. $\bar{a}_0 \neq \bar{0}$), sodass für alle $x \in R$ gilt $\bar{a}_0 \cdot \bar{x} \neq \bar{1}$. Sei

$$J_0 := \{x \cdot a_0 + y \cdot b : x, y \in R \wedge b \in I\}.$$

Dann ist $J_0 \subseteq R$ ein Ideal mit $a_0 \in J_0$ und $1 \notin J_0$. Um $1 \notin J_0$ zu sehen, beachte, dass aus $x \cdot a_0 + y \cdot b = 1$ mit $b \in I$ (d. h. $\overline{y \cdot b} = \bar{0}$), $\bar{x} \cdot \bar{a}_0 = \bar{1}$ folgt, im Widerspruch zu unserer Annahme. Es gilt somit

$$I \underset{a_0 \notin I}{\subsetneq} J_0 \underset{1 \notin J_0}{\subsetneq} R$$

und I ist nicht maximal.

($\Rightarrow$): Sei R/I ein Körper und sei $I \subsetneq J \subseteq R$. Weiter sei $a_0 \in J \setminus I$. Weil R/I ein Körper ist, existiert ein $\bar{x}$ mit $\bar{a}_0 \cdot \bar{x} = \bar{1}$. Das heisst, $a_0 \cdot x = 1 + b$ für ein $b \in I$. Weil $a_0 \in J$, ist mit (I_2) auch $a_0 \cdot x \in J$, und weil $I \subseteq J$, ist $b \in J$. Somit ist mit (I_1) auch $a_0 \cdot x - b = 1 \in J$. Weil $1 \in J$, haben wir $J = R$, und somit ist I ein maximales Ideal. ⊣

Als Folgerung erhalten wir:

KOROLLAR 10.5. *Ein Ideal $m\mathbb{Z} \subseteq \mathbb{Z}$ ist genau dann maximal, wenn m eine Primzahl ist.*