Definition (5.3)

(i) Eine Halbgruppe ist ein Paar $(G, \cdot)$ bestehend aus einer nichtleeren Menge G und einer assoziativen Verknüpfung $\cdot$ auf der Menge G.

(ii) Ein Element $e \in G$ in einer Halbgruppe wird Neutralelement genannt, wenn $g \cdot e = e \cdot g = g$ für alle $g \in G$ erfüllt ist.

(iii) Eine Halbgruppe $(G, \cdot)$, in der ein Neutralelement existiert, wird Monoid genannt.

Definition (5.4)

(i) Ein Element g in einem Monoid $(G, \cdot)$ mit Neutralelement e heißt invertierbar, wenn ein $h \in G$ existierst, so dass die Gleichungen $g \cdot h = h \cdot g = e$ erfüllt sind.

(ii) Eine Gruppe ist ein Monoid, in dem jedes Element invertierbar ist.

(iii) Eine Halbgruppe, und ebenso ein Monoid und eine Gruppe, wird kommutativ oder abelsch genannt, wenn die zugehörige Verknüpfung kommutativ ist.

Definition der Ringe

Definition (5.7)

Ein Ring ist ein Tripel $(R, +, \cdot)$ bestehend aus einer Menge R und zwei Verknüpfungen $+$ und $\cdot$ auf R mit folgenden Eigenschaften.

(i) Das Paar $(R, +)$ ist eine abelsche Gruppe.

(ii) Das Paar $(R, \cdot)$ ist ein abelsches Monoid.

(iii) Es gilt das Distributivgesetz $a(b + c) = ab + ac$ für alle $a, b, c \in R$.

Rechenregeln in Ringen

Proposition (5.8)

Sei $(R, +, \cdot)$ ein Ring, und seien $a, b \in R$. Dann gilt

(i) $-0_R = 0_R$, $-(-a) = a$ und $-(a+b) = (-a) + (-b)$,

(ii) $0_R \cdot a = 0_R$, $a(-b) = (-a)b = -(ab)$ und $ab = (-a)(-b)$,

(iii) $1_R^{-1} = 1_R$, $(a^{-1})^{-1} = a$ und $(ab)^{-1} = a^{-1}b^{-1}$, sofern a und b in $(R, \cdot)$ invertierbar sind.

(iv) Ist R sogar ein Körper, dann folgt aus $ab = 0_R$ immer $a = 0_R$ oder $b = 0_R$.

Beweis von Proposition 5.8:

In einem Monoid $(G, \circ)$ gilt für invertierbare Elemente $a, b \in G$ generell $(a^{-1})^{-1} = a$, $(ab)^{-1} = b^{-1}a^{-1}$. Außerdem ist das Neutralelement des Monoids e invertierbar, und $e^{-1} = e$.

Durch Anwendung dieser Regeln auf das Monoid $(R, +)$ erhalten wir $-0_R = 0_R$, $-(-a) = a$ und $-(a+b) = (-b)+(-a) = (-a)+(-b)$ für alle $a, b \in R$.

$\llcorner (R,+)$ kommutativ

Durch Anwendung der Regeln auf das Monoid $(R, \cdot)$ erhalten wir $1_R^{-1} = 1_R$, $(a^{-1})^{-1} = a$ und $(ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1}$, falls a, b invertierbar in $(R, \cdot)$.

Damit sind (i), (iii) erledigt.

zu (ii) Seien $a, b, c \in R$. Aufgrund der Kommutativität gilt das Distributivgesetz auch „von rechts", d.h.

$$(a+b)\cdot c = c\cdot(a+b) = ca + cb = ac + bc.$$

Weil dies für bel. Ringelemente gilt, folgt

$$0_R \cdot a = (0_R + 0_R)\cdot a = 0_R \cdot a + 0_R \cdot a \Rightarrow$$

$$0_R \cdot a + (-(0_R \cdot a)) = 0_R \cdot a + 0_R \cdot a + (-(0_R \cdot a)) \Rightarrow$$

$$0_R = 0_R \cdot a$$

Überprüfe nun, dass $a(-b)$ das Inverse von ab in $(R,+)$ ist. ($\Rightarrow a(-b) = -ab$)

Tatsächlich gilt $a \cdot (-b) + a \cdot b = a \cdot ((-b)+b) = a \cdot 0_R = 0_R$, $a \cdot b + a \cdot (-b) = a \cdot (-b) + a \cdot b = 0_R$

Der Nachweis von $(-a)b = -(ab)$ läuft analog.

Es folgt $(-a) \cdot (-b) \overset{5.0}{=} -a \cdot (-b) \overset{5.0}{=} -(-ab) \overset{5.0}{=} ab$.

Zu (iv) Angenommen, es gibt Elemente $a, b \in R \setminus \{0_R\}$ mit $a \cdot b = 0_R$. R Körper, $a, b \in R \setminus \{0_R\} \rightarrow a, b$ sind in $(R, \cdot)$ invertierbar $\rightarrow a = a \cdot 1_R = a \cdot b \cdot b^{-1} = 0_R \cdot b^{-1} = 0_R$ ↯ zu $a \neq 0_R$. □

Fragen:

(1) Kann in einem Ring $1_R = 0_R$ gelten?

(2) Ist es möglich, dass 0_R in $(R, \cdot)$ invertierbar ist, also 0_R^{-1} existiert?

Antwort auf beide Fragen: Ja, wenn $R = \{0_R\} = \{1_R\}$ gilt, der Ring also nur aus einem Element besteht.
(Solche Ringe heißen Nullringe.)

Zu (1) Setze $1_R = 0_R$ voraus. Sei $a \in R$.

$$\Rightarrow a = a \cdot 1_R = a \cdot 0_R = 0_R$$

Zu (2) Voraussetzung: Es gibt ein Element 0_R^{-1} mit

$0_R \cdot 0_R^{-1} = 1_R$ Sei $a \in R$. Dann folgt

$a = a \cdot 1_R = a\, 0_R\, 0_R^{-1} = 0_R\, 0_R^{-1} = 1_R$

Anwendung der Gleichung auf $a = 0_R$ liefert $0_R = 1_R$

also: $R = \{0_R\}$. □

Addition und Multiplikation auf $\mathbb{Z}/n\mathbb{Z}$

Erinnerung: Sei $n \in \mathbb{N}$.

- $\mathbb{Z}/n\mathbb{Z} = \{a+n\mathbb{Z} \mid a \in \mathbb{Z}\} = \{0+n\mathbb{Z}, 1+n\mathbb{Z}, ..., (n-1)+n\mathbb{Z}\}$
- Für $a, b \in \mathbb{Z}$ gilt $a + n\mathbb{Z} = b + n\mathbb{Z}$ genau dann, wenn $b - a$ durch n teilbar ist.

Satz (5.9)

Sei $n \in \mathbb{N}$. Dann gibt es eindeutig bestimmte Abbildungen $+ : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ und $\cdot : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ mit

$$(a + n\mathbb{Z}) + (b + n\mathbb{Z}) \quad = \quad (a + b) + n\mathbb{Z}$$

und

$$(a + n\mathbb{Z}) \cdot (b + n\mathbb{Z}) \quad = \quad ab + n\mathbb{Z}$$

für alle $a, b \in \mathbb{Z}$.

Bem: Bei der Definition von Abbildungen auf $\mathbb{Z}/n\mathbb{Z}$ oder $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ kann es leicht zu Fehlern kommen. Beispielsweise gibt es keine Abbildung $f: \mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$ mit $f(a+3\mathbb{Z}) = a+4\mathbb{Z}$ $\forall a \in \mathbb{Z}$.

Angenommen ein solches f existiert. Dann folgt

$1+4\mathbb{Z} = f(1+3\mathbb{Z}) = f(4+3\mathbb{Z}) = 4+4\mathbb{Z}$.

$\Rightarrow 4-1=3$ ist durch 4 teilbar ↯ da $4 \nmid 3$

Beweis von Proposition 5.9

bekannt: $R = \{0, 1, \ldots, n-1\}$ ist ein Repräsentantensystem für $\mathbb{Z}/n\mathbb{Z}$, d.h. jede Restklasse $a + n\mathbb{Z}$ enthält genau ein Element aus R.

Definiere nun $+$ und $\cdot$ auf $\mathbb{Z}/n\mathbb{Z}$ für beliebige $A, B \in \mathbb{Z}/n\mathbb{Z}$ durch

$$A + B = a_0 + b_0 + n\mathbb{Z} \text{ bzw.}$$

$$A \cdot B = a_0 \cdot b_0 + n\mathbb{Z}, \text{ wobei } a_0 \in R$$

den eindeutig best. Repräsentanten von A und $b_0 \in R$ den eindeutig best. Repr. von B bezeichnet.

Sei nun $a, b \in \mathbb{Z}$ vorgegeben. Zu zeigen

$$(a + n\mathbb{Z}) + (b + n\mathbb{Z}) = a + b + n\mathbb{Z}$$
$$(a + n\mathbb{Z}) \cdot (b + n\mathbb{Z}) = a \cdot b + n\mathbb{Z}$$

Division mit Rest liefert $q, q' \in \mathbb{Z}$ und $a_0, b_0 \in \{0, \ldots, n-1\}$ mit $a = qn + a_0$ und $b = q'n + b_0$.
Die Elemente a_0, b_0 sind die Repr. von $a + n\mathbb{Z}$ bzw. $b + n\mathbb{Z}$ in R. Nach Def. gilt also

$$(a + n\mathbb{Z}) + (b + n\mathbb{Z}) = a_0 + b_0 + n\mathbb{Z}$$
$$(a + n\mathbb{Z}) \cdot (b + n\mathbb{Z}) = a_0 b_0 + n\mathbb{Z}$$

z.Zg also: $a+b+n\mathbb{Z} = a_0+b_0+n\mathbb{Z}$ und
$ab+n\mathbb{Z} = a_0b_0+n\mathbb{Z}$, gleichbedeutend damit
ist $n \mid ((a+b)-(a_0+b_0))$ bzw. $n \mid (ab-a_0b_0)$
Dies ist tatsächlich der Fall, denn:
$(a+b)-(a_0+b_0) = (a-a_0)+(b-b_0) = qn+q'n =$
$(q+q')n$ und $ab-a_0b_0 = ab-a_0b+a_0b-a_0b_0$
$= (a-a_0)b + a_0(b-b_0) = qnb + a_0q'n =$
$(qb+a_0q')n$. □

Addition und Multiplikation auf $\mathbb{Z}/4\mathbb{Z}$

Vorgehensweise:

- Um zwei Elemente $a + 4\mathbb{Z}$ und $b + 4\mathbb{Z}$ in $\mathbb{Z}/4\mathbb{Z}$ zu addieren, bilde die Summe $a + b$ und anschließend den Rest von $a + b$ von nach Division durch 4.
- Um zwei Elemente $a + 4\mathbb{Z}$ und $b + 4\mathbb{Z}$ in $\mathbb{Z}/4\mathbb{Z}$ zu multiplizieren, bilde das Produkt ab und anschließend den Rest von ab von nach Division durch 4.

Beispiele:

- $(3 + 4\mathbb{Z}) + (2 + 4\mathbb{Z}) = 5 + 4\mathbb{Z} = 1 + 4\mathbb{Z}$
- $(3 + 4\mathbb{Z}) \cdot (2 + 4\mathbb{Z}) = 6 + 4\mathbb{Z} = 2 + 4\mathbb{Z}$

‘

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{2}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Addition und Multiplikation auf $\mathbb{Z}/7\mathbb{Z}$

Beispiele:

- $(5 + 7\mathbb{Z}) + (4 + 7\mathbb{Z}) = 9 + 7\mathbb{Z} = 2 + 7\mathbb{Z}$
- $(6 + 7\mathbb{Z}) \cdot (4 + 7\mathbb{Z}) = 24 + 7\mathbb{Z} = 3 + 7\mathbb{Z}$

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{6}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{1}$	$\bar{3}$	$\bar{5}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{6}$	$\bar{2}$	$\bar{5}$	$\bar{1}$	$\bar{4}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{1}$	$\bar{5}$	$\bar{2}$	$\bar{6}$	$\bar{3}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{3}$	$\bar{1}$	$\bar{6}$	$\bar{4}$	$\bar{2}$
$\bar{6}$	$\bar{0}$	$\bar{6}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Definition der Restklassenringe

Satz (5.10)

Sei $n \in \mathbb{N}$. Dann bildet das Tripel $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ einen Ring, mit $\bar{0} = 0 + n\mathbb{Z}$ als Null- und $\bar{1} = 1 + n\mathbb{Z}$ als Einselement. Man bezeichnet ihn als Restklassenring modulo n.

Beweis von Satz 5.10 (nur Ansatz)

Alle Rechenregeln übertragen sich von Ring $(\mathbb{Z}, +, \cdot)$ auf $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$, werden also von $\mathbb{Z}$ „geerbt".

überprüfe exemplarisch:

(1) $1+n\mathbb{Z}$ ist Neutralelement in $(\mathbb{Z}/n\mathbb{Z}, \cdot)$

(2) Es gilt das Distributivgesetz.

zu (1) Sei $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$. z.Zg. $\bar{1} \cdot \bar{a} = \bar{a} \cdot \bar{1} = \bar{a}$ (wobei $\bar{1} = 1+n\mathbb{Z}$)

$\bar{a} \in \mathbb{Z}/n\mathbb{Z} \rightarrow \exists a \in \mathbb{Z}$ mit $\bar{a} = a + n\mathbb{Z}$. Dann gilt

$\bar{1} \cdot \bar{a} = (1+n\mathbb{Z}) \cdot (a+n\mathbb{Z}) = 1 \cdot a + n\mathbb{Z} = a + n\mathbb{Z} = \bar{a}$

(Nachweis von $\bar{a} \cdot \bar{1} = \bar{a}$ analog)

zu (2) Seien $\bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}/n\mathbb{Z}$. z.Zg:

$$\bar{a} \cdot (\bar{b} + \bar{c}) = \bar{a} \cdot \bar{b} + \bar{a} \cdot \bar{c}$$

Seien $a, b, c \in \mathbb{Z}$ mit $\bar{a} = a + n\mathbb{Z}$, $\bar{b} = b + n\mathbb{Z}$, $\bar{c} = c + n\mathbb{Z}$. Dann folgt

$$\bar{a} \cdot (\bar{b} + \bar{c}) = (a + n\mathbb{Z}) \cdot ((b + n\mathbb{Z}) + (c + n\mathbb{Z})) =$$

$$(a + n\mathbb{Z}) \cdot ((b + c) + n\mathbb{Z}) = a \cdot (b + c) + n\mathbb{Z} =$$

$$= ab + ac + n\mathbb{Z} = (ab + n\mathbb{Z}) + (ac + n\mathbb{Z}) =$$

$$(a + n\mathbb{Z})(b + n\mathbb{Z}) + (a + n\mathbb{Z}) \cdot (c + n\mathbb{Z}) = \bar{a} \cdot \bar{b} + \bar{a} \cdot \bar{c}.$$

□

Endliche Körper

Lemma (5.11)

Sind $m, n \in \mathbb{N}$ teilerfremd, dann gibt es $a, b \in \mathbb{Z}$ mit $am + bn = 1$.

Satz (5.12)

Für jedes $n \in \mathbb{N}$ ist der Restklassenring $\mathbb{Z}/n\mathbb{Z}$ genau dann ein Körper, wenn n eine Primzahl ist.

Beweis von Satz 5.12:

Sei $n \in \mathbb{N}$. z.Zg: $\mathbb{Z}/n\mathbb{Z}$ ist Körper $\iff$ n ist Primzahl

„$\Longrightarrow$" Ang. n ist keine Primzahl, aber $\mathbb{Z}/n\mathbb{Z}$ ist ein Körper. Dann gibt es zwei Möglichkeiten:

(1) $n = 1$ (2) $\exists\, r, s \in \mathbb{N}$ mit $1 < r, s < n$, $n = rs$

zu (1) Dann gilt $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/1\mathbb{Z} = \{0 + 1\cdot\mathbb{Z}\} = \{0_{\mathbb{Z}/n\mathbb{Z}}\}$

Wäre $\mathbb{Z}/1\mathbb{Z}$ ein Körper, dann müsste $\mathbb{Z}/1\mathbb{Z} \setminus \{0_{\mathbb{Z}/n\mathbb{Z}}\} = \emptyset$ die Menge der bzgl. $\cdot$ invertierbaren Elemente sein. aber: $0_{\mathbb{Z}/n\mathbb{Z}}$ ist aber invertierbar, wg. $0_{\mathbb{Z}/n\mathbb{Z}} \cdot 0_{\mathbb{Z}/n\mathbb{Z}} = 0_{\mathbb{Z}/n\mathbb{Z}} = 1_{\mathbb{Z}/n\mathbb{Z}}$ für $n = 1$, d.h. die Menge der inv. Elemente ist <u>nicht</u> leer ↯.

zu (2) Betrachte $\bar{r} = r + n\mathbb{Z}$, $\bar{s} = s + n\mathbb{Z}$.

Es gilt $\bar{r} \cdot \bar{s} = rs + n\mathbb{Z} = n + n\mathbb{Z} = 0 + n\mathbb{Z} = 0_{\mathbb{Z}/n\mathbb{Z}}$ aber: $\bar{r} \neq 0_{\mathbb{Z}/n\mathbb{Z}}$, $\bar{s} \neq 0_{\mathbb{Z}/n\mathbb{Z}}$: da n kein Teiler von $r = 0$ oder $s = 0$ ist.

Da $\mathbb{Z}/n\mathbb{Z}$ ein Körper ist, ist so etwas nicht möglich.

Kehrwerte in den Körpern $\mathbb{F}_7$ und $\mathbb{F}_{13}$

Notation: Ist p eine Primzahl, dann verwendet man für $\mathbb{Z}/p\mathbb{Z}$ auch die Bezeichnung $\mathbb{F}_p$. (Der Buchstabe $\mathbb{F}$ steht für die englische Übersetzung des algebraischen Begriffs „Körper“, „field“.)

Durch probeweises Multiplizieren findet man die folgenden Kehrwerte in $\mathbb{F}_7$.

a	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
a^{-1}	–	$\bar{1}$	$\bar{4}$	$\bar{5}$	$\bar{2}$	$\bar{3}$	$\bar{6}$

Kehrwerte in $\mathbb{F}_{13}$

a	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{8}$	$\bar{9}$	$\overline{10}$	$\overline{11}$	$\overline{12}$
a^{-1}	–	$\bar{1}$	$\bar{7}$	$\bar{9}$	$\overline{10}$	$\bar{8}$	$\overline{11}$	$\bar{2}$	$\bar{5}$	$\bar{3}$	$\bar{4}$	$\bar{6}$	$\overline{12}$