Skriptum zur Vorlesung

Algebra

Erstellt von Christopher Frei
nach den Vorlesungsunterlagen von Sophie Frisch
unter Verwendung von Teilen eines Skriptums von Stephan Wagner

WS 2007/2008

Inhaltsverzeichnis

Teil I

Ringe

1 Definitionen und Beispiele

Definition 1.1 Eine Menge $R \neq \emptyset$ zusammen mit zwei inneren Operationen $+ : R \times R \to R$ (genannt Addition) und $\cdot : R \times R \to R$ (genannt Multiplikation) heißt *Ring*, wenn gilt:

- $(R, +)$ ist eine kommutative Gruppe (das neutrale Element bezüglich $+$ wird mit 0 bzw. 0_R bezeichnet)
- $(R, \cdot)$ ist eine Halbgruppe
- $\forall a, b, c \in R: \ a \cdot (b + c) = a \cdot b + a \cdot c \wedge (a + b) \cdot c = a \cdot c + b \cdot c$ („*Distributivität*“)

Man schreibt: $(R, +, \cdot)$ ist Ring (oder: R ist Ring).

Definition 1.2

- $(R, +, \cdot)$ heißt *Ring mit Eins*, wenn $(R, \cdot)$ ein Monoid ist; das neutrale Element bezüglich $\cdot$ wird mit 1 (bzw. 1_R) bezeichnet.
- R heißt *kommutativer Ring*, wenn $(R, \cdot)$ kommutativ ist.
- Ein Ring heißt *endlicher Ring*, wenn $\exists n \in \mathbb{N}$ mit $|R| = n$.

Im Folgenden seien alle Ringe (wenn nicht ausdrücklich anders vereinbart) Ringe mit 1.

Definition 1.3 Für $(R, +)$ und $(R, \cdot)$ werden die für Gruppen und Monoide eingeführten Schreibweisen verwendet:

- Das Inverse von a bezüglich $+$ wird als $-a$ geschrieben; $a - b := a + (-b)$
  Das Inverse von a bezüglich $\cdot$ wird als a^{-1} geschrieben;
- *Vielfache*: für $a \in R, n \in \mathbb{Z}$ definiert man

$$na := \begin{cases} a + \ldots + a & n > 0 \\ 0 & n = 0 \\ (-a) + \ldots + (-a) & n < 0 \end{cases}$$

- *Potenzen*: $a^n := a \cdot \ldots \cdot a$ für $n \in \mathbb{N}$; falls R Ring mit Eins ist, $a^0 := 1$; falls R Ring mit Eins ist und a ein Inverses a^{-1} hat, $a^{-n} := a^{-1} \cdot \ldots \cdot a^{-1}$

BEISPIEL: $(\mathbb{Z}, +, \cdot)$ ist ein kommutativer Ring, jeder Körper ($\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_p$) ist ein kommutativer Ring. $\mathbb{Z}_n = {}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$ sind kommutative Ringe.

$\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ und $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ (Gaußsche ganze Zahlen) sind kommutative Ringe. (jeweils $\subset \mathbb{C}$)

$(2\mathbb{Z}, +, \cdot)$ ist ein kommutativer Ring ohne 1. (allgemein $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$)

Für einen Körper K (z.B. $K = \mathbb{Q}$ oder $K = \mathbb{R}$) bilden die Matrizen $M_n(K)$ mit der üblichen Matrizenaddition und -multiplikation einen Ring; für $n > 1$ ist er nichtkommutativ. Unter den Matrizenringen gibt es auch endliche nichtkommutative Ringe: $M_n(\mathbb{Z}_p)$ (für eine Primzahl p) ist ein endlicher nichtkommutativer Ring.

Sei $(G, +)$ eine kommutative Gruppe; $\mathrm{End}(G) = \{\varphi : G \to G \,|\, \varphi(g + h) = \varphi(g) + \varphi(h)\}$ (die Menge der Endomorphismen von G) bildet mit den Operationen $+$, definiert durch $(\varphi + \psi)(g) = \varphi(g) + \psi(g)\ \forall g \in G$, sowie $\circ$, definiert durch $(\varphi \circ \psi)(g) = \varphi(\psi(g))\ \forall g \in G$, einen Ring.

Die oberen Dreiecksmatrizen in $M_n(K)$ bilden einen nichtkommutativen Ring.

Die strikten oberen Dreiecksmatrizen in $M_n(K)$ bilden einen nichtkommutativen Ring ohne 1.

Satz 1.4 (Rechenregeln für Ringe) *Wenn $(R, +, \cdot)$ ein Ring ist, dann gilt:*

1. $\forall a \in R: \ a \cdot 0_R = 0_R \cdot a = 0_R$ (*Bemerkung: dies ist eine andere Aussage als die Definition des 0-ten Vielfachen von a durch $0a := 0_R$!*)
2. $\forall a, b, c \in R: \ a \cdot (b - c) = a \cdot b - a \cdot c$; $\forall a, b, c \in R: \ (a - b) \cdot c = a \cdot c - b \cdot c$
3. $(-a) \cdot b = a \cdot (-b) = -(a \cdot b)$; $(-a) \cdot (-b) = a \cdot b$
4. $(-a)^n = (-1)^n a^n = \begin{cases} a^n & n \text{ gerade} \\ -a^n & n \text{ ungerade} \end{cases}$ (*hierbei ist $(-1)^n$ in $\mathbb{Z}$ zu verstehen*)
5. *für $n, m \in \mathbb{Z}$, $a, b \in R$:* $(na) \cdot (mb) = (m \cdot n)(a \cdot b)$
6. *wenn R ein Einselement 1_R hat, dann ist $\forall n \in \mathbb{Z}$, $a \in R$:* $na = (n1_R) \cdot a = a \cdot (n1_R)$
7. *verallgemeinerte Distributivität:*

$$\left(\sum_{i=1}^{n} a_i\right)\left(\sum_{j=1}^{m} b_j\right) = \sum_{i=1}^{n}\sum_{j=1}^{m} a_i b_j \left(= \sum_{j=1}^{m}\sum_{i=1}^{n} a_i b_j\right)$$

$$\begin{aligned} (a_1 + \ldots + a_n) \cdot (b_1 + \ldots + b_m) &= (a_1 \cdot b_1 + \ldots a_1 \cdot b_m) + \ldots + (a_n \cdot b_1 + \ldots a_n \cdot b_m) \\ &= (a_1 \cdot b_1 + \ldots a_n \cdot b_1) + \ldots + (a_1 \cdot b_m + \ldots a_n \cdot b_m) \end{aligned}$$

Beweis: 1. $(a \cdot 0_R) = a \cdot (0_R + 0_R) = a \cdot 0_R + a \cdot 0_R$; durch Addition von $-(a \cdot 0_R)$ erhält man $0_R = a \cdot 0_R$. Analog folgt $0_R = 0_R \cdot a$.
Rest: als Übung. ∎

Definition 1.5 Sei $(R, +, \cdot)$ ein Ring mit Eins.

- $a \in R$ heißt *rechtsinvertierbar* (*Rechtseinheit*), wenn

$$\exists a_r \in R \text{ mit } a \cdot a_r = 1_R$$

- $a \in R$ heißt *linksinvertierbar* (*Linkseinheit*), wenn

$$\exists a_l \in R \text{ mit } a_l \cdot a = 1_R$$

a_r heißt dann Rechtsinverses von a, a_l Linksinverses.

Definition 1.6 Sei R ein Ring.

- $a \in R$ heißt *linkskürzbar*, wenn $\forall b, c \in R\ ab = ac \Rightarrow b = c$.
- $a \in R$ heißt *rechtskürzbar*, wenn $\forall b, c \in R\ ba = ca \Rightarrow b = c$.

Lemma 1.7 Sei R ein Ring und $a \in R$.

- a linksinvertierbar $\Longrightarrow$ a linkskürzbar
- a rechtsinvertierbar $\Longrightarrow$ a rechtskürzbar

Beweis: Sei a_l das Linksinverse von a, d.h. $a_l a = 1$; multipliziert man nun $ab = ac$ von links mit a_l, dann folgt $a_l ab = 1b = b = c = 1c = a_l ac$. Die zweite Behauptung folgt analog. ∎

Bemerkung: Die Umkehrung gilt nicht: In $\mathbb{Z}$ sind nur 1 und -1 invertierbar, aber jedes Element $\neq 0$ ist kürzbar.

Bemerkung: In einem kommutativen Ring sind die Begriffe linksinvertierbar und rechtsinvertierbar äquivalent, genauso die Begriffe linkskürzbar und rechtskürzbar. Auch im Folgenden sind alle Eigenschaften, die links und rechts definiert werden, für kommutative Ringe äquivalent.

Definition 1.8 Sei R ein Ring.

- $b \in R$ heißt *Linksnullteiler*, wenn $\exists c \in R \setminus \{0\}$ mit $b \cdot c = 0$.
- $b \in R$ heißt *Rechtsnullteiler*, wenn $\exists c \in R \setminus \{0\}$ mit $c \cdot b = 0$.

BEMERKUNG: 0 ist Links- und Rechtsnullteiler, sofern $R \neq \{0\}$.

Lemma 1.9 Sei R ein Ring und $a \in R$.

- a linksinvertierbar $\Longrightarrow$ a kein Linksnullteiler
- a rechtsinvertierbar $\Longrightarrow$ a kein Rechtsnullteiler

Beweis: Sei a_l das Linksinverse von a, d.h. $a_l a = 1$; Sei $b \in R$ mit $ab = 0$. Dann gilt $b = 1b = a_l ab = a_l 0 = 0$. Die zweite Behauptung folgt analog. ∎

BEISPIEL: In $\mathbb{Z}$: 0 ist der einzige Nullteiler, 1 und -1 sind die invertierbaren Elemente und alle Elemente $\in \mathbb{Z} \setminus \{-1, 0, 1\}$ sind weder Nullteiler noch invertierbar.

Lemma 1.10 In einem beliebigen Ring R ist für $a \in R$ äquivalent:

1. L_a injektiv
2. a linkskürzbar
3. a kein Linksnullteiler

wobei $L_a : R \to R$, $L_a(x) = a \cdot x$ (Linkstranslation von a)

Beweis:
(1) $\Leftrightarrow$ (2): L_a injektiv heißt $ab = ac \Rightarrow b = c$.
(2) $\Rightarrow$ (3): $a \cdot b = 0$, d.h. $a \cdot b = a \cdot 0$. Aus a linkskürzbar folgt $b = 0$. Somit ist a kein Linksnullteiler.
(3) $\Rightarrow$ (2): $ab = ac \Rightarrow a(b - c) = 0$. Aus a kein Linksnullteiler folgt $b - c = 0$, also $b = c$. ∎

Lemma 1.11 In einem beliebigen Ring R ist für $a \in R$ äquivalent:

1. R_a injektiv
2. a rechtskürzbar
3. a kein Rechtsnullteiler

wobei $R_a : R \to R$, $R_a(x) = x \cdot a$ (Rechtstranslation von a)

Beweis: Analog zu Lemma 1.10. ∎

Lemma 1.12 Sei R ein Ring und $a \in R$.

1. a linksinvertierbar $\iff R_a$ surjektiv
2. a rechtsinvertierbar $\iff L_a$ surjektiv

Beweis:
($\Rightarrow$) $\exists a_l : \ a_l a = 1$; für $b \in R$ folgt damit $b = b1 = ba_l a = R_a(ba_l)$, also ist R_a surjektiv.
($\Leftarrow$) $\exists a' \in R$ mit $R_a(a') = 1$, d.h. $a'a = 1$. Damit ist a' Linksinverses von a.
(2) folgt analog. ∎

Definition 1.13 Sei R ein Ring und $a \in R$.

- a heißt *invertierbar* oder *Einheit*, wenn a links- und rechtsinvertierbar ist.
- $a \in R$ heißt *Nullteiler*, wenn a Links- oder Rechtsnullteiler ist.

Bemerkung: Wenn $a \in R$ invertierbar ist, gibt es ein eindeutiges $a^{-1} \in R$, sodass $a \cdot a^{-1} = a^{-1} \cdot a = 1_R$ (siehe das entsprechende Resultat für Monoide).

Bemerkung: Für einen endlichen Ring R gilt für alle $a \in R$: a Einheit oder a Nullteiler (und nicht beides).

Beispiel: In $M_n(K)$ gilt:

$$A \text{ invertierbar } \iff \operatorname{rang}(A) = n \ (\iff \det(A) \neq 0)$$

$$A \text{ Nullteiler } \iff \operatorname{rang}(A) < n \ (\iff \det(A) = 0)$$

Definition 1.14 Sei R ein Ring. $a \in R$ heißt *nilpotent*, wenn $\exists n \in \mathbb{N}$ mit $a^n = 0$.
$(a \cdot \ldots \cdot a = 0)$

Bemerkung: $a^n = 0$, d.h. a ist nilpotent in einem Ring, ist nicht zu verwechseln mit $a^n = e$, d.h. a hat endliche Ordnung in einer Gruppe!

Beispiel: In $M_n(K)$ sind die strikten oberen Dreiecksmatrizen nilpotente Elemente.

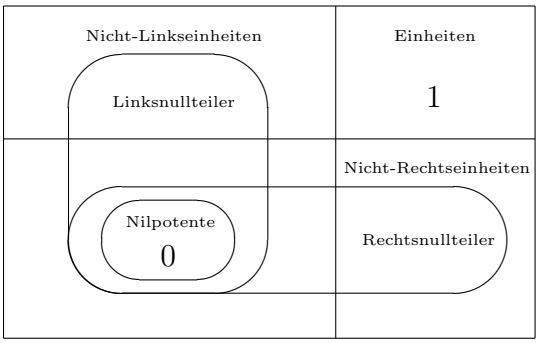
Beispiel: In $Z_n = {}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$ gilt für $\overline{k} = k + n\mathbb{Z}$:

- $\overline{k}$ nilpotent $\iff \forall p$ prim mit $p|n$ gilt $p|k$
- $\overline{k}$ Nullteiler $\iff \exists p$ prim mit $p|n$ und $p|k$ (d.h. $\operatorname{ggT}(k, n) \neq 1$)

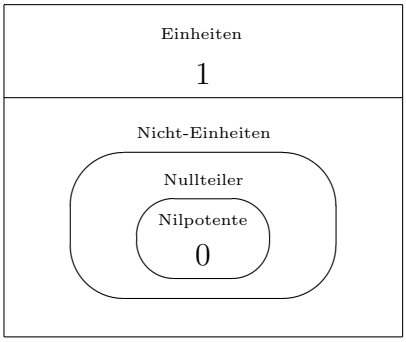
Proposition 1.15 Sei $R \neq \{0\}$. Dann gilt: a nilpotent $\Rightarrow$ a Nullteiler (sogar Rechts- und Linksnullteiler).

Beweis: Sei $n \in \mathbb{N}$ minimal, sodass $a^n = 0$. Wenn $n = 1$, dann ist $a = 0$, also wegen $R \neq \{0\}$ ein Nullteiler. Wenn $n > 1$, dann gilt $0 = a^n = a \cdot a^{n-1} = a^{n-1} \cdot a$ und $a^{n-1} \neq 0$.■

Ring mit 1



Kommutativer Ring mit 1



Beispiel: In $\mathbb{Z}_6$ sind $\overline{2}$ und $\overline{3}$ Nullteiler, denn $\overline{2} \cdot \overline{3} = \overline{3} \cdot \overline{2} = \overline{6} = \overline{0}$, aber $\overline{2}$ und $\overline{3}$ sind nicht nilpotent: $\overline{2}^n = \overline{2^n} = \overline{0}$ würde gelten, wenn $6|2^n$; dies ist jedoch unmöglich.

Definition 1.16 Sei R ein Ring mit Eins. Dann ist

$$E(R) = R^* := \{a \in R \,|\, a \text{ invertierbar}\}$$

eine Gruppe, die *Einheitengruppe* von R (wir wissen bereits: die invertierbaren Elemente eines Monoids bilden eine Gruppe).

Beispiel: Sei K ein Körper, z.B. $K = \mathbb{R}$, V ein K-Vektorraum. Die Menge der Endomorphismen auf V,

$$\mathrm{End}_K(V) := \{L : V \to V \,|\, L(x+y) = L(x) + L(y), L(kx) = kL(x)\ \forall x, y \in V,\ k \in K\}$$

bildet einen Ring bezüglich der Operationen $+$, $\circ$ (nicht kommutativ).

Definition 1.17 Seien R, S Ringe. Eine Funktion $f : R \to S$ heißt *Ringhomomorphismus*, wenn f sowohl ein Gruppenhomomorphismus $f : (R, +) \to (S, +)$, als auch ein Halbgruppenhomomorphismus $f : (R, \cdot) \to (S, \cdot)$ ist, d.h.
$f(a + b) = f(a) + f(b)$ und
$f(a \cdot b) = f(a) \cdot f(b)$.

Ein bijektiver Ringhomomorphismus heißt *Ringisomorphismus*.

Bemerkung: Sei V ein n-dimensionaler K-Vektorraum, dann gilt $\mathrm{End}_K(V) \simeq M_n(K)$ (isomorph als Ringe). Es gibt für jede Wahl einer Basis B von V einen Ringisomorphismus $f_B : \mathrm{End}_K(V) \to M_n(K)$, nämlich $f_B(\varphi) = [\varphi]_B$ (die Matrixdarstellung von φ bezüglich B).

Beispiel: Sei V ein K-Vektorraum. In $\mathrm{End}_K(V)$ gilt:

1. L rechtsinvertierbar $\iff$ L surjektiv
2. L linksinvertierbar $\iff$ L injektiv

Beweis: 1. ($\Leftarrow$) Sei L surjektiv, B eine Basis von V. Für jedes $b \in B$ wähle $b' \in L^{-1}(b)$ ($\neq \emptyset$); setze $\widetilde{L}(b) = b'$ für $b \in B$ ($\exists!$ lineare Abbildung $\widetilde{L} : V \to V$, die das erfüllt). Dann gilt $\forall b \in B$ $(L \circ \widetilde{L})(b) = L(b') = b$, also ist $L \circ \widetilde{L}$ eine lineare Abbildung, die auf einer Basis B $L \circ \widetilde{L} = \mathrm{id}$ erfüllt. Somit gilt $L \circ \widetilde{L} = \mathrm{id}$.
($\Rightarrow$) Wir wissen bereits: L hat (als Funktion) eine Rechtsinverse $\Rightarrow$ L ist surjektiv.

2. ($\Leftarrow$) Sei L injektiv, B eine Basis von V. Dann ist $B' = \{L(b) = b' \mid b \in B\}$ eine linear unabhängige Menge:
Seien $b'_1 = L(b_1), \ldots, b'_n = L(b_n) \in B'$ und $c_1 b'_1 + \ldots + c_n b'_n = 0$. Dann folgt:
$$0 = c_1 b'_1 + \ldots + c_n b'_n = c_1 L(b_1) + \ldots + c_n L(b_n) = L(c_1 b_1 + \ldots + c_n b_n)$$
Da L injektiv ist, muss daher $c_1 b_1 + \ldots + c_n b_n = 0$ sein, also $c_i = 0$ $\forall i$, da B eine Basis ist. Folglich ist B' linear unabhängig.
Nun kann man B' zu einer Basis C ergänzen und eine Funktion $\widetilde{L} : V \to V$ auf der Basis C definieren: für $b' \in B'$ sei $\widetilde{L}(b') = b$, wobei b das eindeutig bestimmte Element von B mit $L(b) = b'$ sei; für $c \in C \setminus B$ sei $\widetilde{L}(c)$ beliebig, z.B. $\widetilde{L}(c) = 0$. Dann folgt für $b \in B$ $\widetilde{L}(L(b)) = \widetilde{L}(b') = b$, also muss $\widetilde{L} \circ L = \mathrm{id}$ sein.
($\Rightarrow$) Wir wissen bereits: L hat (als Funktion) eine Linksinverse $\Rightarrow$ L ist injektiv. ∎

Beispiel: Sei $(G, +)$ eine kommutative Gruppe, $f \in \mathrm{End}(G)$. Dann gilt: f linksinvertierbar in $(\mathrm{End}(G), +, \circ) \Rightarrow f$ ist injektiv. Die Umkehrung gilt jedoch nicht:
Wähle z.B. $G = (\mathbb{Z}, +)$, $f \in \mathrm{End}(\mathbb{Z})$ als $f(x) = 2x$. Dann ist f injektiv, hat aber keine Linksinverse: aus $g(f(x)) = x$ würde etwa für $x = 1$ folgen
$$g(f(1)) = g(2) = g(1 + 1) = g(1) + g(1) = 1,$$
was in den ganzen Zahlen unmöglich ist.

Übungsbeispiele

Übung 1: Sei R ein kommutativer Ring.

(i) Wenn $a \in R$ ein Nullteiler und $b \in R$ beliebig, dann ist ab ein Nullteiler.

(ii) Die Menge der Nicht-Nullteiler von R ist multiplikativ abgeschlossen, d.h., wenn a kein Nullteiler und b kein Nullteiler, dann ist auch ab kein Nullteiler.

Übung 2: Sei $(R, +, \cdot)$ ein Ring und a, b, $c \in R$. Zeigen Sie

(i) $(-a) \cdot b = -(a \cdot b) = a \cdot (-b) \quad$ und $\quad (-a) \cdot (-b) = a \cdot b$

(ii) $a \cdot (b - c) = a \cdot b - a \cdot c \quad$ und $\quad (a - b) \cdot c = a \cdot c - b \cdot c$

Übung 3: Sei $(R, +, \cdot)$ ein Ring, a, $b \in R$, $k \in \mathbb{N}_0$ und n, $m \in \mathbb{Z}$. Zeigen Sie

(i) $(-a)^k = (-1)^k a^k$

(ii) $(na) \cdot (mb) = (n \cdot m)(a \cdot b) \quad$ (Hier ist $n \cdot m$ das Produkt in $\mathbb{Z}$.)

(iii) Wenn R ein Einselement 1_R hat, dann ist $\; na = (n1_R) \cdot a = a \cdot (n1_R)$.

Übung 4: Sei $(G, +)$ eine kommutative Gruppe und

$$\mathrm{End}(G) := \{f : G \to G \mid f(a + b) = f(a) + f(b)\}$$

die Menge aller Endomorphismen von G. Dann ist $(\mathrm{End}(G), +, \circ)$ mit $(f + g)(x) = f(x) + g(x)$ und $(f \circ g)(x) = f(g(x))$ ein Ring. Welche Ringaxiome werden nicht erfüllt, wenn $(G, +)$ nicht kommutativ ist, bzw. wenn man beliebige Funktionen $f : G \to G$ statt Gruppenhomomorphismen betrachtet?

Übung 5: Sei $R \neq \{0\}$ ein endlicher nullteilerfreier Ring. Dann ist R ein Schiefkörper. (Bemerkung: Tatsächlich ist — nach dem Satz von Wedderburn — R dann sogar ein Körper.)

2 Ideale

Definition 2.1 Sei S ein Ring und $R \subseteq S$. R heißt *Unterring* von S, geschrieben $R \leq S$, wenn R bezüglich $+, \cdot$ abgeschlossen ist (d.h. $a, b \in R \Rightarrow a + b \in R,\ a \cdot b \in R$), und R bezüglich der Einschränkungen von $+$ und $\cdot$ auf $R \times R \to R$ die Ringaxiome erfüllt.

Bemerkung: Aus der Definition eines Unterrings folgt nicht, dass $1_R = 1_S$.

Beispiel: $M_{n-1}(K)$, der Ring der $(n-1) \times (n-1)$-Matrizen über K, kann isomorph in $M_n(K)$ eingebettet werden, indem man rechts und unten 0-en hinzufügt.

$R = \{\begin{pmatrix} A & 0 \\ 0 & 0 \end{pmatrix} \mid A \in M_n(K)\}$ ist ein Unterring von $M_n(K)$, mit $R \simeq M_{n-1}(K)$. R ist also ein Ring mit 1, enthält jedoch nicht $I_n = 1_{M_n(K)}$.

Bemerkung: An diesem Beispiel sieht man auch, dass ein Ringhomomorphismus $f : R \to S$ nicht $f(1) = 1$ erfüllen muss (auch nicht, wenn beide Ringe ein Einselement haben).

$f : M_{n-1}(K) \to M_n(K)$, $f(A) = \begin{pmatrix} A & 0 \\ 0 & 0 \end{pmatrix}$ erfüllt nicht $f(I_{n-1}) = I_n$.

Definition 2.2 Sei R ein Ring, $I \subseteq R$. Wenn $(I, +)$ eine Untergruppe von $(R, +)$ ist und $\forall i \in I, r \in R\ ir \in I$, dann heißt I *Rechtsideal* von R. Wenn $(I, +)$ eine Untergruppe von $(R, +)$ ist und $\forall i \in I, r \in R\ ri \in I$, dann heißt I *Linksideal* von R. Wenn I Links- und Rechtsideal ist, dann heißt I *Ideal* von R, geschrieben $I \trianglelefteq R$.

Bemerkung: Eine Untergruppe $(I, +) \leq (R, +)$ ist

- Unterring, wenn $a, b \in I \ \Rightarrow\ ab \in I$ (schwächste Bedingung)
- Linksideal, wenn $r \in R, b \in I \ \Rightarrow\ rb \in I$
- Rechtsideal, wenn $a \in I, r \in R \ \Rightarrow\ ar \in I$
- Ideal, wenn $r \in R, i \in I \ \Rightarrow\ ri \in I$ und $ir \in I$ (stärkste Bedingung)

Daher ist jedes Links- oder Rechtsideal Unterring, aber nicht umgekehrt. In einem kommutativen Ring ist jedes Linksideal auch Rechtsideal und umgekehrt. Jeder Ring hat die trivialen Ideale $\{0\}$ und R.

Bemerkung: Sei $I \subseteq R$. Wenn $I \neq \emptyset$, $a, b \in I \ \Rightarrow\ a - b \in I$ und $r \in R, i \in I \ \Rightarrow\ ri, ir \in I$ gilt, dann ist I ein Ideal.

BEISPIEL: Als Ideale von $(\mathbb{Z}, +, \cdot)$ kommen nur Untergruppen von $(\mathbb{Z}, +)$ in Frage, diese sind von der Form $\{0\}$ oder $n\mathbb{Z}$ für ein $n \in \mathbb{N}$. $n\mathbb{Z}$ ist auch ein Ideal: wenn $r \in \mathbb{Z}$ und $i = nl \in n\mathbb{Z}$ ist, dann ist $ri = ir = nrl \in n\mathbb{Z}$. Also sind die Ideale von $\mathbb{Z}$ $\{0\}$ und $n\mathbb{Z}$ $(n \in \mathbb{N})$.

BEISPIEL: $\mathbb{Z} \leq \mathbb{Q}$ ist ein Unterring, aber weder Links- noch Rechtsideal: $1 \in \mathbb{Z}, \frac{1}{2} \in \mathbb{Q}$, aber $1 \cdot \frac{1}{2} = \frac{1}{2} \notin \mathbb{Z}$.

BEISPIEL: In $M_n(K)$: Sei $N_{i_1,\ldots,i_k}$ die Teilmenge aller Matrizen, in deren i_1-ter, …, i_k-ter Zeile nur 0 steht. $N_{i_i,\ldots,i_k}$ ist ein Rechtsideal von $M_n(K)$ ($A \cdot B = C$ und i-te Zeile von A ist $(0, \ldots, 0) \Rightarrow i$-te Zeile von C ist $(0, \ldots, 0)$).

Sei $N^{i_1,\ldots,i_k}$ die Teilmenge aller Matrizen, in deren i_1-ter, …, i_k-ter Spalte nur 0 steht. $N^{i_i,\ldots,i_k}$ ist ein Linksideal von $M_n(K)$ ($A \cdot B = C$ und i-te Spalte von B ist Nullvektor $\Rightarrow i$-te Spalte von C ist Nullvektor).

BEISPIEL: Sei K ein Körper und $M_n(K)$ der Matrizenring über diesem Körper. Dann ist jedes Linksideal von der Form $\mathcal{L}_A := \{MA \mid M \in M_n(K)\}$ für eine Matrix $A \in M_n(K)$.
Ebenso ist jedes Rechtsideal von der Form $\mathcal{R}_B := \{BM \mid M \in M_n(K)\}$ für eine Matrix $B \in M_n(K)$.
Daher hat $M_n(K)$ nur die trivialen Ideale $\{0\}$ und $M_n(K)$ (Beweise als Übung).

Lemma 2.3 Sei R ein Ring und für $i \in I$ sei A_i ein Unterring (Rechtsideal/Linksideal/Ideal). Dann ist $\bigcap_{i \in I} A_i$ ein Unterring (Rechtsideal/Linksideal/ Ideal).

Beweis: Wir wissen bereits, dass $(A_i, +) \leq (R, +) \Rightarrow (\bigcap_{i \in I} A_i, +) \leq (R, +)$. Wenn jedes A_i Unterring ist, also $\forall i \in I\ (r, s \in A_i \Rightarrow rs \in A_i)$ gilt, und $r, s \in \bigcap_{i \in I} A_i$ sind, dann ist $\forall i \in I\ r, s \in A_i$, also $\forall i \in I\ rs \in A_i$ und somit $rs \in \bigcap_{i \in I} A_i$. Daher ist A_i ein Unterring. Für Rechtsideal/Linksideale/Ideale läuft der Beweis analog. ∎

Definition 2.4 Sei R ein Ring und $X \subseteq R$. Das von X *erzeugte Ideal* ist

$$(X) := \bigcap_{I \trianglelefteq R, X \subseteq I} I$$

Der von X *erzeugte Unterring* ist

$$[X] := \bigcap_{S \leq R, X \subseteq S} S$$

Weiters ist das von X erzeugte Linksideal $\bigcap_{I \text{ Linksideal}, X \subseteq I} I$, das von X erzeugte Rechtsideal $\bigcap_{I \text{ Rechtsideal}, X \subseteq I} I$.

Definition 2.5 Ein *Hauptideal* ist ein von einem Element a erzeugtes Ideal. Man schreibt (a) statt $(\{a\})$.

Satz 2.6 (Hauptideale) *Sei $(R,+,\cdot)$ ein Ring, $a \in R$. Dann gilt:*

1. $(a) = \{na + ra + as + \sum_{i=1}^{m} r_i a s_i \,|\, n \in \mathbb{Z}, r, s, r_i, s_i \in R, m \in \mathbb{N}_0\}$
2. *Für einen Ring mit Eins:* $(a) = \{\sum_{i=1}^{m} r_i a s_i \,|\, r_i, s_i \in R, m \in \mathbb{N}_0\}$
3. *Für einen kommutativen Ring:* $(a) = Ra + \mathbb{Z}a = \{ra + na \,|\, r \in R, n \in \mathbb{Z}\}$
4. *Für einen kommutativen Ring mit Eins:* $(a) = Ra = \{ra \,|\, r \in R\} =$ $= aR = \{ar \,|\, r \in R\}$

Beweis:
Ad 1.: Sei $M = \{na + ra + as + \sum_{i=1}^{m} r_i a s_i \,|\, n \in \mathbb{Z}, r, s, r_i, s_i \in R, m \in \mathbb{N}_0\}$. Dann gilt:

i. Für alle Ideale $I \trianglelefteq R$ mit $a \in I$ gilt $M \subseteq I$, denn: $(I,+) \leq (R,+) \;\Rightarrow\; na \in I$; I ist bezüglich Multiplikation von links und rechts abgeschlossen $\Rightarrow\; ra, as, r_i a s_i \in I$; I ist bezüglich $+$ abgeschlossen $\Rightarrow$ jedes Element der Form $na + ra + as + \sum_{i=1}^{m} r_i a s_i$ muss in I enthalten sein, also $M \subseteq I$.

ii. M ist ein Ideal von R und $a \in M$:
Zweiteres ist unmittelbar klar, da $a = 1_{\mathbb{Z}}a + 0_R a + a0_R + 0_R a 0_R \in M$. Damit ist außerdem $M \neq \emptyset$.
Es seien $na + ra + as + \sum_{i=1}^{m} r_i a s_i$ und $n'a + r'a + as' + \sum_{i=1}^{m'} r'_i a s'_i$ zwei Elemente aus M. Dann ist ihre Differenz

$$(n - n')a + (r - r')a + a(s - s') + \sum_{i=1}^{m+m'} r''_i a s''_i \in M$$

Seien weiters $b = na + ra + as + \sum_{i=1}^{m} r_i a s_i \in M$ und $r' \in R$. Dann ist ihr Produkt

$$\begin{aligned} r'b &= r'(na + ra + as + \sum_{i=1}^{m} r_i a s_i) \\ &= r'(na) + r'ra + ras + \sum_{i=1}^{m} r' r_i a s_i \\ &= (nr' + r'r)a + \sum_{i=1}^{m'} r'_i a s'_i \in M \end{aligned}$$

Analog ist auch $br' \in M$.

Wegen ii. kommt M unter den Idealen, die a enthalten, vor. Daher ist $(a) = \bigcap_{I \trianglelefteq R, a \in I} I \subseteq M$. Wegen i. wiederum muss $M \subseteq \bigcap_{I \trianglelefteq R, a \in I} I = (a)$ sein, also folgt $M = (a)$.

Ad 2.-4.: Die entsprechenden Mengen sind jedenfalls nach 1. in (a) enthalten. Sie umfassen jedoch aufgrund der zusätzlichen Bedingungen auch ganz (a):

- Ad 2.: R hat ein Einselement $\Rightarrow na = (n1_R)a1_R$, $ra = ra1_R$, $as = 1_R as$
- Ad 3.: R ist kommutativ $\Rightarrow as = sa$, $\sum_{i=1}^m r_i a s_i = (\sum_{i=1}^m r_i s_i)a$
- Ad 4.: R ist kommutativer Ring mit Einselement $\Rightarrow na = (n1_R)a$, $as = sa$, $\sum_{i=1}^m r_i a s_i = (\sum_{i=1}^m r_i s_i)a$

Daher ist $na + ra + as + \sum_{i=1}^m r_i a s_i$ jeweils von der angegebenen Form. ∎

Beispiel: In $\mathbb{Z}$ ist jedes Ideal ein Hauptideal $(n) = n\mathbb{Z}$.

Definition 2.7 (Addition und Multiplikation von Mengen)
Sei R ein Ring und $A, B \subseteq R$. Dann definiert man:

1. $A + B := \{a + b \,|\, a \in A, b \in B\}$
2. $AB := \{a_1 b_1 + \ldots + a_n b_n \,|\, n \in \mathbb{N}, a_i \in A, b_i \in B\}$

Durch diese Definition ist AB bezüglich $+$ abgeschlossen.

Bemerkung: Statt $\{a\}B$ für ein $a \in R$ schreibt man aB, analog $Ab = A\{b\}$. Wegen der Distributivität gilt $aR = \{ar_1 + \ldots + ar_n \,|\, r_i \in R\} = \{ar \,|\, r \in R\}$ und analog $Ra = \{ra \,|\, r \in R\}$. In diesem Sinne ist dann für einen Ring mit Eins $(a) = RaR$ und für einen kommutativen Ring mit Eins $(a) = aR = Ra$.

Lemma 2.8 Seien I, J Ideale von R. Dann sind auch $I + J$ und IJ Ideale von R.

Beweis:
ad 1) I, J sind Untergruppen von $(R, +)$, also ist auch $I + J$ eine Untergruppe von $(R, +)$ (die von $I \cup J$ erzeugte Untergruppe von $(R, +)$). Sei $i + j \in I + J$ und $r \in R$, dann ist $r(i + j) = ri + rj \in I + J$, analog $(i + j)r \in I + J$. Also ist $I + J$ ein Ideal.

ad 2) $IJ = \{i_1 j_1 + \ldots + i_n j_n \,|\, i_k \in I, j_k \in J\}$ ist bezüglich $+, -$ abgeschlossen
$(-(i_1 j_1 + \ldots + i_k j_k) = (-i_1)j_1 + \ldots + (-i_k)j_k)$. Somit ist IJ eine Untergruppe von $(R, +)$. Weil I bezüglich Multiplikation mit $r \in R$ von links abgeschlossen ist, und J bezüglich Multiplikation mit $r \in R$ von rechts abgeschlossen ist, folgt: IJ ist abgeschlossen bezüglich Multiplikation mir $r \in R$ von links oder rechts. ∎

Satz 2.9 (Rechenregeln für Ideale) *Seien $A_1, \ldots, A_n, A, B, C$ Ideale. Dann gilt:*

1. $A + (B + C) = (A + B) + C$
2. $A(BC) = (AB)C$
3. $A(B + C) = AB + AC$, $(A + B)C = AC + BC$
4. $(A_1 + \ldots + A_n)B = A_1B + \ldots + A_nB$, $B(A_1 + \ldots + A_n) = BA_1 + \ldots + BA_n$
5. *Wenn R ein Ring mit Eins ist, dann gilt für alle Linksideale I von R $RI = I$ und für alle Rechtsideale J von R $JR = J$.*

Beweis: als Übung. ∎

Bemerkung: Wozu man Ideale eigentlich braucht:

1. Man kann Faktorstrukturen bilden
2. Ideale sind genau die Teilmengen, die als Kern von Ringhomomorphismen auftreten

Faktorringe

Satz 2.10 *Sei $(R, +, \cdot)$ ein Ring und $I \trianglelefteq R$. Für $a \in R$ sei*

$$a + I := \{a + i \,|\, i \in I\} = \{b \in R \,|\, b - a \in I\}$$

(die Nebenklasse von a bezüglich $(I, +) \leq (R, +)$) und

$$R/I := \{a + I \,|\, a \in R\}.$$

Dann bildet R/I mit der Addition $(a + I) + (b + I) = (a + b) + I$ und der Multiplikation $(a + I) \cdot (b + I) = (a \cdot b) + I$ einen Ring.
Wenn R kommutativ ist, dann auch R/I; wenn R ein Ring mit einem Einselement 1_R ist, dann ist $1_R + I$ das Einselement von R/I. Weiters ist $\pi : R \to R/I$ mit $\pi(a) = a + I$ ein Ringepimorphismus (die kanonische Projektion) mit $\operatorname{Ker} \pi = I$.

Beweis: Wir wissen bereits, dass $(R/I, +)$ eine kommutative Gruppe ist. Zu zeigen ist zunächst, dass $(R/I, \cdot)$ eine Halbgruppe ist und das Distributivgesetz erfüllt ist:

- $\cdot$ ist wohldefiniert: sei $a+I = a'+I$, $b+I = b'+I$, d.h. $a-a' = i \in I$ und $b-b' = j \in I$. Dann ist $a'b' - ab = (a + i)(b + j) - ab = ab + aj + ib + ij - ab = aj + ib + ij \in I$, also $a'b' + I = ab + I$.
- Die Assoziativität von $\cdot$ und die Distributivität ergeben sich aus den entsprechenden Bedingungen für R. Ebenso ist R/I kommutativ, wenn R kommutativ ist. Falls R ein Einselement hat, ist $(a + I)(1 + I) = a1 + I = a + I = 1a + I = (1 + I)(a + I)$, also muss $1 + I$ Einselement in R/I sein.

Es ist bereits bekannt, dass $\pi : R \to {}^{R}/_{I}$ ein Gruppenepimorphismus bezüglich $+$ ist, wobei $\operatorname{Ker}\pi = I$. Weil zudem $\pi(ab) = ab + I = (a+I)(b+I) = \pi(a)\pi(b)$ gilt, ist π auch Ringhomomorphismus. ∎

BEISPIEL: Sei $n\mathbb{Z}$ ein Ideal von $\mathbb{Z}$. Der Faktorring ${}^{\mathbb{Z}}/_{n\mathbb{Z}}$ sind die „ganzen Zahlen modulo n". Die Elemente von ${}^{\mathbb{Z}}/_{n\mathbb{Z}}$ sind die Nebenklassen von $n\mathbb{Z}$ in $(\mathbb{Z}, +)$, $k + n\mathbb{Z}$ für $k \in \mathbb{Z}$ (es gibt genau n verschiedene).

$k + n\mathbb{Z} = l + n\mathbb{Z} \iff n \mid (k-l)$, z.B. sind $0 + n\mathbb{Z}, 1 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}$ alle Restklassen.

Addition: $(k + n\mathbb{Z}) + (l + n\mathbb{Z}) = (k + l) + n\mathbb{Z}$
Multiplikation: $(k + n\mathbb{Z}) \cdot (l + n\mathbb{Z}) = k \cdot l + n\mathbb{Z}$

Wenn wir voraussetzen, dass Elemente in $\mathbb{Z}$ eine eindeutige Primfaktorzerlegung haben, dann sehen wir: Die Nullteiler in ${}^{\mathbb{Z}}/_{n\mathbb{Z}}$ sind genau die Klassen $k + n\mathbb{Z}$ mit $\operatorname{ggT}(k, n) \neq 1$ ($\exists p$ prim mit $p \mid k$, $p \mid n$). Die Einheiten sind genau die Klassen $k + n\mathbb{Z}$ mit $\operatorname{ggT}(k, n) = 1$.

Übungsbeispiele

Übung 6:
Sei R ein Ring. Für A, $B \subseteq R$ sei $AB = \{a_1b_1 + \ldots + a_nb_n \mid n \in \mathbb{N}, a_i \in A, b_i \in B\}$ und $A + B = \{a + b \mid a \in A, b \in B\}$. Sei $a \in R$, und A, B, $C \subseteq R$. Dann gilt:

(i) $A + (B + C) = (A + B) + C$

(ii) $A(BC) = (AB)C$

(iii) Wenn $0 \in B$ und $0 \in C$, dann gilt $(B+C)A = BA+CA$ und $A(B+C) = AB+AC$

Übung 7: Sei R ein Ring, a, $b \in R$. Dann gilt $(ab) \subseteq (a)(b)$.
Wenn R kommutativ ist, dann gilt $(ab) = (a)(b)$.

Übung 8: Sei K ein Körper. Der Ring $R = M_n(K)$ hat kein (beidseitiges) Ideal außer R und (0). Hinweis: Matrizen von rechts und links mit verschiedenen Matrixeinheiten E_{ij} (und mit Skalarmatrizen) multiplizieren. Die Matrixeinheit E_{ij} hat als Eintragungen nur 0, ausser einem Einser an der Stelle (i, j).

Übung 9: Seien I, J Ideale eines Ringes R. Dann ist $I + J$ das von $I \cup J$ erzeugte Ideal von R.

Übung 10: Seien I, J Ideale von R. Dann gilt $IJ \subseteq I \cap J$. Es gilt im Allgemeinen nicht $IJ = I \cap J$; finden Sie ein Gegenbeispiel für Ideale von $\mathbb{Z}$.

Übung 11: Seien I, J Ideale eines kommutativen Rings mit 1. Wenn $I + J = R$, dann gilt $IJ = I \cap J$. (Hinweis: $(I \cap J)R$ betrachten.) Was bedeutet das für Ideale von $\mathbb{Z}$?

Übung 12: Seien $a_1, \ldots, a_n \in R$, R ein kommutativer Ring mit 1, dann ist

$$(a_1, \ldots, a_n) = a_1R + \ldots + a_nR.$$

3 Homomorphismen

Definition 3.1 Seien R und S Ringe. Der *Kern* eines Ringhomomorphismus $f : R \to S$ ist definiert als

$$\operatorname{Ker} f := \{a \in R \,|\, f(a) = 0_S\} = f^{-1}(0_S)$$

Das *Bild* von f wiederum ist

$$\operatorname{Im} f := \{f(a) \,|\, a \in R\} = f(R)$$

Lemma 3.2 Sei $f : R \to S$ ein Ringhomomorphismus, dann ist $\operatorname{Im} f$ ein Unterring von S und $\operatorname{Ker} f$ ein Ideal von R.

Beweis: $\operatorname{Im} f$ ist bezüglich $+, -, \cdot$ abgeschlossen und daher ein Unterring von S.

$\operatorname{Ker} f \leq (R, +)$ als Kern des Gruppenhomomorphismus $f : (R, +) \to (S, +)$. Sei $r \in R, i \in \operatorname{Ker} f$. Dann gilt $f(ri) = f(r) \cdot f(i) = f(r) \cdot 0 = 0$ und $f(ir) = f(i) \cdot f(r) = 0 \cdot f(r) = 0$. Somit sind ir und $ri \in \operatorname{Ker} f$. ∎

Definition 3.3 Ein surjektiver Ringhomomorphismus heißt – wie für Gruppen – *Epimorphismus*, ein injektiver *Monomorphismus*, ein bijektiver *Isomorphismus*, einer, der R auf sich abbildet, *Endomorphismus*, und ein bijektiver Endomorphismus heißt *Automorphismus*.

Satz 3.4 (Homomorphiesatz, 1. Isomorphiesatz) *Sei $f : R \to S$ ein Ringhomomorphismus. Dann ist $\overline{f} : {}^{R}\!/_{\operatorname{Ker} f} \to \operatorname{Im} f$ mit $\overline{f}(r + \operatorname{Ker} f) = f(r)$ ein Ringisomorphismus. Insbesondere ist ${}^{R}\!/_{\operatorname{Ker} f}$ isomorph zu $\operatorname{Im} f$.*

Beweis: Wir setzen $K := \operatorname{Ker} f$.

- $\overline{f}$ ist wohldefiniert: $a' \in a + K \;\Rightarrow\; a' = a + k$ für ein $k \in K \;\Rightarrow\; f(a') = f(a) + f(k) = f(a) + 0 = f(a)$
- $\overline{f}$ ist offensichtlich surjektiv, und zudem auch injektiv: $\overline{f}(a + K) = \overline{f}(b + K) \;\Rightarrow\; f(a) = f(b) \;\Rightarrow f(a - b) = 0 \;\Rightarrow a - b \in K \;\Rightarrow\; a + K = b + K$
- $\overline{f}$ ist Ringhomomorphismus:

$$\overline{f}((a+K)+(b+K)) = \overline{f}(a+b+K) = f(a+b) = f(a)+f(b) = \overline{f}(a+K)+\overline{f}(b+K)$$

$$\overline{f}((a + K)(b + K)) = \overline{f}(ab + K) = f(ab) = f(a)f(b) = \overline{f}(a + K)\overline{f}(b + K)$$

Beispiel: $n\mathbb{Z} \trianglelefteq \mathbb{Z}$; $\pi : \mathbb{Z} \to {}^{\mathbb{Z}}\!/_{n\mathbb{Z}} = \mathbb{Z}_n$ mit $\pi(m) = \overline{m} = m + \mathbb{Z}$ ist auch Ringepimorphismus.

BEMERKUNG: Wir haben bereits gesehen, dass der Kern jedes Ringhomomorphismus ein Ideal ist. Auch die Umkehrung gilt: Jedes Ideal ist Kern eines Ringhomomorphismus, nämlich der kanonischen Projektion von R auf ${}^{R}/_{I}$,

$$\pi : R \to {}^{\mathrm{R}}/_{\mathrm{I}}, \quad \pi(r) = r + I.$$

Definition 3.5 Ein Ring S heißt *homomorphes Bild* eines Rings R, wenn es einen surjektiven Ringhomomorphismus $f : R \to S$ gibt.

BEMERKUNG: Bis auf Isomorphie sind homomorphe Bilder dasselbe, wie Faktorringe: Der Faktorring ${}^{R}/_{I}$ ist homomorphes Bild wegen $\pi : R \to {}^{R}/_{I}$. Ein homomorphes Bild ist isomorph zu einem Faktorring via 1.Isomorphiesatz: $f : R \to S$ surjektiver Ringhomomorphismus $\Rightarrow S \simeq {}^{R}/_{\mathrm{Ker}\, f}$.

BEMERKUNG: Sei S Unterring von R und $I \trianglelefteq R$. Dann ist $S \cap I \trianglelefteq S$ (die Einschränkung von I auf S).

Satz 3.6 (2. Isomorphiesatz) *Sei R ein Ring, S ein Unterring von R und I ein Ideal von R. Dann gilt*

$$ {}^{S}/_{(I \cap S)} \simeq {}^{(S+I)}/_{I}$$

wobei $f : {}^{S}/_{(I \cap S)} \to {}^{(S+I)}/_{I}$ mit $f(s + I \cap S) = s + I$ der Isomorphismus ist.

BEMERKUNG: Die Idee dahinter: Man möchte ${}^{S}/_{I}$ bilden, aber $I \not\subseteq S$. Die zwei Möglichkeiten das zu reparieren liefern isomorphe Ringe: ${}^{S}/_{(I \cap S)}$ und ${}^{(S+I)}/_{I}$ sind isomorph.

Beweis (des Satzes): $g : S \to {}^{(S+I)}/_{I}$, $g(s) = s + I$ ist ein surjektiver Ringhomomorphismus. (${}^{(S+I)}/_{I}$ ist der Unterring von ${}^{R}/_{I}$ bestehend aus allen Klassen mit einem Repräsentanten in $S + I$. Diese Klassen haben auch einen Repräsentanten in S: $(s + i) + I = s + I$.)

Es gilt: $\mathrm{Ker}\, g = S \cap I$: Sei $s \in S$ mit $s + I = g(S) = 0 + I = I$, dann folgt $s \in I$, also $\mathrm{Ker}\, g \subseteq S \cap I$. Sei umgekehrt $s \in S \cap I$, dann gilt $g(s) = s + I = I$, also $s \in \mathrm{Ker}\, g$ und $S \cap I \subseteq \mathrm{Ker}\, g$.

Nach dem 1. Isomorphiesatz gilt ${}^{S}/_{\mathrm{Ker}\, g} \simeq \mathrm{Im}\, g$, also ${}^{S}/_{(S \cap I)} \simeq {}^{(S+I)}/_{I}$ via

$\overline{g}(s + (S \cap I)) = g(s) = s + I.$ ∎

BEISPIEL: $R = \mathbb{Z}$, $S = 12\mathbb{Z}$, $I = 15\mathbb{Z}$.

$12\mathbb{Z} \cap 15\mathbb{Z} = 60\mathbb{Z}$ $(n\mathbb{Z} \cap m\mathbb{Z} = \mathrm{kgV}\,(n,m)\mathbb{Z})$
$12\mathbb{Z} + 15\mathbb{Z} = 3\mathbb{Z}$ $(n\mathbb{Z} + m\mathbb{Z} = \mathrm{ggT}\,(n,m)\mathbb{Z})$

$$12\mathbb{Z}/60\mathbb{Z} \simeq 3\mathbb{Z}/15\mathbb{Z}$$
$$k + 60\mathbb{Z} \mapsto k + 15\mathbb{Z}.$$

BEMERKUNG: 2. Isomorphiesatz gilt auch für Gruppen (auch nichtkommutative):

Sei G eine Gruppe, $H \leq G$, $N \trianglelefteq G$. Dann gilt:

$$H/(H \cap N) \simeq HN/N$$

via $f(h(H \cap N)) = hN$.

Formale Voraussetzungen überprüfen:

- $H \leq G$, $N \trianglelefteq G \;\Rightarrow\; H \cap N \trianglelefteq H$
- $H \leq G$, $N \trianglelefteq G \;\Rightarrow\; HN \leq G$, nämlich $HN = \langle H \cup N \rangle$, die von $H \cup N$ erzeugte Untergruppe.

BEMERKUNG: Allgemein gilt: Wenn H, N Untergruppen von G sind, dann

$$\langle H \cup N \rangle = HN \Longleftrightarrow HN = NH,$$

wobei $HN = \{hn \,|\, h \in H, n \in N\}$ und $NH = \{nh \,|\, n \in N, h \in H\}$.

Wenn N Normalteiler von G ist, dann $\forall h \in G : hN = Nh$, somit
$\forall h \in H\ \forall n \in N\ \exists n' \in N :\ hn = n'h$, also $HN \subseteq NH$
$\forall h \in H\ \forall n \in N\ \exists n'' \in N :\ nh = hn''$, also $NH \subseteq HN$

Beweis (2. Isomorphiesatz für Gruppen): $g : H \to HN/N$, $g(h) = hN$ ist ein surjektiver Gruppenhomomorphismus. $\ker g = H \cap N$. 1. Isomorphiesatz: $H/H \cap N \simeq HN/N$. ∎

Proposition 3.7 (Homomorphismen und Ideale) Sei $f : R \to S$ ein Ringhomomorphismus. Dann gilt:

- $T \leq R \;\Rightarrow\; f(T) \leq S$
- $U \leq S \;\Rightarrow\; f^{-1}(U) \leq R$
- $I \trianglelefteq R \;\Rightarrow\; f(I) \trianglelefteq f(R)$ (im Allgemeinen aber nicht $f(I) \trianglelefteq S$!)
- $J \trianglelefteq S \;\Rightarrow\; f^{-1}(J) \trianglelefteq R$

Beweis: als Übung. ∎

BEMERKUNG: Sei $I \trianglelefteq R$ und $\pi : R \to {}^{R}/_{I}$, $\pi(r) = r + I$ die kanonische Projektion. Sei $S \leq R$, dann gilt $\pi(S) \leq {}^{R}/_{I}$.

$\pi(S) = \{s + I \mid s \in S\} = {}^{(S+I)}/_{I}$ ($S + I$ ist der kleinste Unterring von R, der S und I enthält.)

Wenn $J \trianglelefteq R$, dann $\pi(J) \trianglelefteq {}^{R}/_{I}$ ($= \operatorname{Im}\pi$). $\pi(J) = \{j + I \mid j \in J\} = {}^{(J+I)}/_{I}$

Insbesondere, wenn $S \leq R$ mit $I \subseteq S$, dann $\pi(S) = {}^{S}/_{I} \leq {}^{R}/_{I}$, und wenn $J \trianglelefteq R$ mit $I \subseteq J$, dann $\pi(J) = {}^{J}/_{I} \trianglelefteq {}^{R}/_{I}$.

Lemma 3.8 Sei $f : R \to S$ ein Ringhomomorphismus. Dann gilt:

$$X \subseteq R \implies f^{-1}(f(X)) = X + \operatorname{Ker} f$$

$$Y \subseteq S \implies f(f^{-1}(Y)) = Y \cap \operatorname{Im} f$$

Beweis: Dies gilt bereits, weil f ein Gruppenhomomorphismus bezüglich $+$. ∎

Satz 3.9 (3. Isomorphiesatz) *Sei R ein Ring, I ein Ideal von R und $\pi : R \to {}^{R}/_{I}$ sei die kanonische Projektion.*

Dann ist eine Bijektion zwischen allen Unterringen von R, die I enthalten und allen Unterringen von ${}^{R}/_{I}$ gegeben durch

$$S \mapsto \pi(S) = {}^{S}/_{I}$$

mit der Umkehrabbildung

$$T \mapsto \pi^{-1}(T),$$

und genauso für die Ideale von R, die I enthalten und alle Ideale von ${}^{R}/_{I}$.

Außerdem gilt für $S \leq R$, $J \trianglelefteq R$ mit $I \subseteq J \subseteq S$: ${}^{J}/_{I} \trianglelefteq {}^{S}/_{I}$ und

$$ {}^{S}/_{I} \Big/ {}^{J}/_{I} \simeq {}^{S}/_{J}, $$

wobei der Isomorphismus gegeben ist, durch $(s + I) + {}^{J}/_{I} \mapsto s + J$.

Beweis: 1)
$S \leq R \Rightarrow \pi(S) \leq {}^{R}/_{I}$
$T \leq {}^{R}/_{I} \Rightarrow \pi^{-1}(T) \leq R$ und $\pi^{-1}(T)$ enthält $\pi^{-1}(0) = \ker(\pi)$.
$\varphi : \{S \leq R \mid I \subseteq S\} \to \{T \mid T \leq {}^{R}/_{I}\}$; $\varphi(S) = \pi(S)$ und
$\psi : \{T \mid T \leq {}^{R}/_{I}\} \to \{S \leq R \mid I \subseteq S\}$; $\psi(T) = \pi^{-1}(T)$ sind also als Abbildungen wohldefiniert. Zu zeigen ist: $\varphi \circ \psi = \mathrm{id}$ und $\psi \circ \varphi = \mathrm{id}$.

Für $T \leq {}^{R}\!/_{I}$ gilt:

$$\varphi(\psi(T)) = \pi(\pi^{-1}(T)) = T \cap \operatorname{Im}\pi = T \cap {}^{\mathrm{R}}\!/_{\mathrm{I}} = T.$$

Für $S \leq R$ mit $I \subseteq S$ gilt:

$$\psi(\varphi(S)) = \pi^{-1}(\pi(S)) = S + \ker\pi = S + I = S.$$

Genauso bilden auch die Einschränkungen von φ, ψ auf

$$\{J \mid J \trianglelefteq R, I \subseteq J\} \text{ bzw. } \{L \mid L \trianglelefteq {}^{\mathrm{R}}\!/_{\mathrm{I}}\}$$

eine Bijektion.

2)
Seien $I \subseteq J \subseteq S \subseteq R$, mit I, J Ideale von R, S Unterring von R. Zu zeigen ist:

$${}^{\mathrm{S}}\!/_{\mathrm{I}} \Big/ {}^{\mathrm{J}}\!/_{\mathrm{I}} \simeq {}^{\mathrm{S}}\!/_{\mathrm{J}} \text{ (isomorph als Ringe).}$$

Sei $f : {}^{S}\!/_{I} \to {}^{S}\!/_{J}$; $f(s+I) = s+J$. f ist wohldefiniert, weil $I \subseteq J$. f ist offensichtlich ein surjektiver Ringhomomorphismus.

$$s + I \in \ker f \Leftrightarrow s + J = J \Leftrightarrow s \in J \Leftrightarrow s + I \in {}^{\mathrm{J}}\!/_{\mathrm{I}}$$

Also gilt $\ker f = {}^{J}\!/_{I}$ und nach dem 1. Isomorphiesatz ist:

$$\overline{f} : {}^{\mathrm{S}}\!/_{\mathrm{I}} \Big/ {}^{\mathrm{J}}\!/_{\mathrm{I}} \to {}^{\mathrm{S}}\!/_{\mathrm{J}} \,;\; f((s+I) + {}^{\mathrm{J}}\!/_{\mathrm{I}}) = s + J$$

ein Isomorphismus. ∎

4 Teilbarkeit in kommutativen Ringen

Definition 4.1 Sei R ein kommutativer Ring, $a, b \in R$. a *teilt* b (geschrieben $a \mid b$), wenn es ein $c \in R$ mit $ac = b$ gibt. a heißt dann ein *Teiler* von b, b ein *Vielfaches* von a.

Beispiel: $2 \mid 6$ in $\mathbb{Z}$, $2 \nmid 3$ in $\mathbb{Z}$, aber $2 \mid 3$ in $\mathbb{Q}$ $(2 * \frac{3}{2} = 3)$

Bemerkung: Es gilt:

1. $\forall a \in R$: $a \mid 0$, da $a \cdot 0 = 0$.
2. $\forall a \in R$: $1 \mid a$, da $1 \cdot a = a$. Auch für alle $b \in E(R)$ gilt $\forall a \in R$: $b \mid a$, da $b \cdot (b^{-1}a) = a$.
3. a ist Einheit $\iff a \mid 1$

Bemerkung: Wenn R ein kommutativer Ring mit 1 ist, dann gilt

$$\forall a \in R : (a) = aR = \{ac \mid c \in R\}.$$

Das von a erzeugte Hauptideal besteht also genau aus den Vielfachen von a. $a \mid b$ ist äquivalent zu $b \in (a)$.

Lemma 4.2 $a \mid b \iff (b) \subseteq (a)$

Beweis: $a \mid b \Rightarrow \exists c \in R : \ ac = b$, also $b \in (a)$. Da (a) ein Ideal ist mit $b \in (a)$, folgt auch $(b) \subseteq (a)$. Wenn umgekehrt $(b) \subseteq (a)$, dann ist insbesondere auch $b \in (a)$, d.h. $\exists c \in R : \ b = ca$, und somit $a \mid b$. ∎

Korollar 4.3 Sei R ein kommutativer Ring, $a, b \in R$. Dann gilt

$$a \mid b \wedge b \mid a \iff (a) = (b).$$

Definition 4.4 R heißt *nullteilerfrei*, wenn R keine Nullteiler außer 0 enthält.

Definition 4.5 Ein *Integritätsbereich* ist ein nullteilerfreier kommutativer Ring mit Eins $R \neq \{0\}$.

Definition 4.6 Ein *Schiefkörper* ist ein Ring mit Eins $R \neq \{0\}$, in dem jedes Element außer 0 invertierbar ist.

Definition 4.7 Ein *Körper* ist ein kommutativer Schiefkörper.

Lemma 4.8 In einem Integritätsbereich gilt:

$$a \mid b \wedge b \mid a \iff \exists \text{ Einheit } u \in R : a = ub.$$

Beweis: ($\Leftarrow$) gilt in jedem kommutativen Ring: $a = ub \Rightarrow b \mid a$ und $u^{-1}a = b \Rightarrow a \mid b$.

($\Rightarrow$) $\exists c, d \in R: \ ac = b, bd = a$. Es folgt $b = ac = bdc$, also $b(1 - dc) = 0$. Falls $b = 0$, dann gilt auch $a = 0$ und somit $a = b$. Falls $b \neq 0$, ist b kein Nullteiler (Integritätsbereich), somit ist b kürzbar. Aus $1 - dc = 0$ folgt $dc = 1$, also sind d, c Einheiten. ∎

Definition 4.9 Sei R ein kommutativer Ring. $a, b \in R$, sodass $\exists$ Einheit u mit $a = ub$, heißen *assoziiert*.

Bemerkung: In beliebigen kommutativen Ringen sind

- $a \sim b \ :\Leftrightarrow \ (a \mid b \wedge b \mid a)$
- $a \approx b \ :\Leftrightarrow \ \exists$ Einheit u: $a = ub$

Äquivalenzrelationen und es gilt: $a \approx b \Rightarrow a \sim b$.

Lemma 4.10 Für Teilbarkeit gilt:

- $a \mid b \wedge b \mid c \Rightarrow a \mid c$ (Transitivität)
- $a \mid a$ (Reflexivität)
- $a \mid b \wedge b \mid a \Rightarrow (a) = (b)$ (Symmetrie)

Somit ist Teilbarkeit eine Ordnungsrelation auf Hauptidealen. ($a \mid b \Leftrightarrow (b) \subseteq (a)$)

Definition 4.11 Sei R ein kommutativer Ring, $a, b \in R$. Ein Element $d \in R$ heißt *größter gemeinsamer Teiler* von a und b, wenn gilt:

- $d \mid a \wedge d \mid b$
- $\forall c \in R : (c \mid a \wedge c \mid b \Rightarrow c \mid d)$

Bemerkung: Im Allgemeinen muss es keinen ggT geben.

Bemerkung: Wenn d größter gemeinsamer Teiler von a und b ist und $d \sim d'$, dann ist auch d' größter gemeinsamer Teiler von a und b. Wenn umgekehrt d, d' beide größte gemeinsame Teiler sind, dann gilt $d \sim d'$ (Beweis als Übung).

Der größte gemeinsame Teiler ist also bis auf $\sim$ (gegenseitiges Teilen) eindeutig bestimmt, man schreibt $d \sim \mathrm{ggT}(a, b)$, $d \in \mathrm{ggT}(a, b)$, oder auch $d = \mathrm{ggT}(a, b)$, obwohl d nur ein möglicher ggT ist.

BEMERKUNG (PATHOLOGISCHE FÄLLE DES ggT): Falls $a = 0, b \neq 0$, dann ist $b = \text{ggT}(0, b)$, denn jedes Ringelement c teilt 0 ($0 \cdot c = 0$). Die gemeinsamen Teiler von 0 und b sind also die Teiler von b.

Falls $a = b = 0$, dann gilt $0 = \text{ggT}(0, 0)$.

Definition 4.12 Sei R ein kommutativer Ring, $a_1, \ldots, a_n \in R$. $d \in R$ heißt *größter gemeinsamer Teiler* von $a_1, \ldots, a_n$, wenn gilt:

- $\forall i: \ d \,|\, a_i$
- $\forall c \in R$ mit $\forall i: \ c \,|\, a_i$ gilt $c \,|\, d$.

BEMERKUNG: Wenn in R zu je 2 Elementen ein ggT existiert, dann auch zu endlich vielen: $\text{ggT}(a_1, \text{ggT}(a_2, \text{ggT}(\ldots, \text{ggT}(a_{n-1}, a_n))))$ ist ein ggT von $a_1, \ldots, a_n$.

Übungsbeispiele

Übung 13: Wenn in einem kommutativen Ring mit 1 gilt $(a, b) = (d)$ (d.h., das von a und b erzeugte Ideal lässt sich von einem einzelnen Element d erzeugen), dann ist d ein ggT von a und b.

Übung 14: In einem kommutativen Ring R mit 1 sei d ein grösster gemeinsamer Teiler von a und b.

(i) Wenn für ein $d' \in R$ gilt $d \mid d'$ und $d' \mid d$, dann ist auch d' ggT von a, b.

(ii) Wenn umgekehrt c ein ggT von a und b ist, dann gilt $d \mid c$ und $c \mid d$.

5 Euklidische Ringe

Definition 5.1 Sei R ein kommutativer Ring. R heißt *Euklidischer Ring*, wenn es eine „*Rangfunktion*“ $\rho : R \setminus \{0\} \to \mathbb{N}_0$ gibt, sodass gilt:
$\forall a, b \in R$ mit $b \neq 0$ $\exists q, r \in R$ mit $a = qb + r$ und $r = 0 \vee \rho(r) < \rho(b)$ („Division mit Rest“).
Ein Integritätsbereich, der zugleich Euklidischer Ring ist, heißt *Euklidischer Bereich*.

Beispiel: $\mathbb{Z}$ ist ein Euklidischer Bereich, $\rho(n) = |n|$; Die Elemente $x \in \mathbb{N}_0$ mit $x < |b|$ bilden ein Repräsentantensystem von $\mathbb{Z}/b\mathbb{Z}$. Ein beliebiges $a \in \mathbb{Z}$ ist in einer Klasse $x + b\mathbb{Z}$ für ein $0 \leq x < b$. Somit $a = qb + x$, mit $0 \leq x < b$.

Beispiel: Für einen Körper K ist $K[X]$, der Polynomring mit Koeffizienten in K ein Euklidischer Ring mit $\rho(f) = \deg f$, der Grad des Polynoms. Für $f, g \in K[X]$, $g \neq 0$, $\exists q, r \in K[X]: \ f = qg + r$ und $r = 0$ oder $\deg r < \deg g$.

Euklidischer Algorithmus

Für gegebene a, b in einem euklidischen Ring R liefert der euklidische Algorithmus einen ggT d von a und b. Weiters liefert der Algorithmus $\alpha, \beta \in R$ mit $d = \alpha a + \beta b$.

Es seien $a \neq 0, b \neq 0$ und $\rho(a) \geq \rho(b)$. Wir definieren induktiv Folgen q_i, r_i für $i \geq -1$:

$r_{-1} := a; \ r_0 := b$.
Durch Division mit Rest bekommt man q_0 und r_1: $a = q_0 b + r_1$ ($r_1 = 0$ oder $\rho(r_1) < \rho(b)$).
Im nächsten Schritt: $b = q_1 r_1 + r_2$ (mit $r_2 = 0$ oder $\rho(r_2) < \rho(r_1)$).

Allgemein: Wenn $r_{-1}, r_0, \ldots, r_k$ bereits definiert sind, erhält man q_k, r_{k+1} durch

$$r_{k-1} = q_k r_k + r_{k+1} \text{ (mit } r_{k+1} = 0 \text{ oder } \rho(r_{k+1}) < \rho(r_k)).$$

Schließlich muss für ein n gelten, dass $r_{n+1} = 0$, da sonst $\rho(a) \geq \rho(b) > \rho(r_1) > \rho(r_2) > \ldots$ eine strikt absteigende unendliche Folge natürlicher Zahlen wäre.

Behauptung: Für das minimale n mit $r_{n+1} = 0$ gilt: r_n ist ein ggT von a und b.

Beweis: Wir zeigen:

1. $\forall i : r_n$ teilt r_i (insbesondere also $r_n | r_{-1} = a$ und $r_n | r_0 = b$)
2. jedes c, das a und b teilt, teilt auch alle r_i (insbesondere also $c | r_n$)

ad 1) Induktion von n abwärts: $r_n | r_{n-1}$, da $r_{n-1} = q_n r_n$ (wegen $r_{n+1} = 0$). Wenn $r_n | r_k$ und $r_n | r_{k-1}$, dann folgt auch $r_n | r_{k-2}$, da $r_{k-2} = q_{k-1} r_{k-1} + r_k$.

ad 2) $c | a \wedge c | b \Rightarrow c | r_1$, da $r_1 = a - q_0 b$. Wenn $c | r_{k-1}$ und $c | r_k$, dann gilt auch $c | r_{k+1}$, wegen $r_{k+1} = r_{k-1} - q_k r_k$. ∎

Jetzt bestimmen wir noch α und β, sodass $r_n = \alpha a + \beta b$. Wir definieren Folgen α_i, β_i für $i \geq -1$, sodass $\alpha_i a + \beta_i b = r_i$.

$a = r_{-1} = 1 \cdot a + 0 \cdot b \Rightarrow \alpha_{-1} = 1,\ \beta_{-1} = 0$
$b = r_0 = 0 \cdot a + 1 \cdot b \Rightarrow \alpha_0 = 0,\ \beta_0 = 1$

Angenommen $\alpha_{-1}, \ldots, \alpha_k$ und $\beta_{-1}, \ldots, \beta_k$ sind bereits definiert.

$$r_{k+1} = r_{k-1} - q_k r_k = \alpha_{k-1} a + \beta_{k-1} b - q_k \alpha_k a - q_k \beta_k b = (\alpha_{k-1} - q_k \alpha_k) a + (\beta_{k-1} - q_k \beta_k) b$$

Wir setzen also

$$\alpha_{k+1} = \alpha_{k-1} - q_k \alpha_k \text{ und } \beta_{k+1} = \beta_{k-1} - q_k \beta_k,$$

dann gilt $r_{k+1} = \alpha_{k+1} a + \beta_{k+1} b$.

Schließlich bekommt man $\alpha := \alpha_n$ und $\beta := \beta_n$ mit $\alpha a + \beta b = r_n$.

Insgesamt ergibt sich also folgendes Schema:

i	-1	0	1	$\ldots$
r_i	a	b	r_1	$\ldots$
q_i		q_0	q_1	$\ldots$
α_i	1	0	α_1	$\ldots$
β_i	0	1	β_1	$\ldots$

wobei:

$$r_{k-1} = q_k r_k + r_{k+1} \text{ Division mit Rest}$$
$$\alpha_{k+1} = \alpha_{k-1} - q_k \alpha_k$$
$$\beta_{k+1} = \beta_{k-1} - q_k \beta_k$$

und

$$\alpha_n a + \beta_n b = r_n = \mathrm{ggT}(a, b),$$

wobei n minimal ist, sodass $r_{n+1} = 0$.

Satz 5.2 *Sei R ein Euklidischer Ring, $a, b \in R$.*

1. $\exists d \in R :$ *d ist* ggT *von a und b*
2. $\exists \alpha, \beta \in R :\ d = \alpha a + \beta b$
3. *Es gibt ein effektives Verfahren, um d, α, β zu berechnen (Euklidischer Algorithmus).*

Bemerkung: 1), 2) gelten schon in Hauptidealringen.

Definition 5.3 Ein Ring R mit Eins heißt *Hauptidealring*, wenn

$$\forall I \trianglelefteq R\ \exists a \in R :\ I = (a).$$

Satz 5.4 *Jeder Euklidische Ring ist ein Hauptidealring.*

Beweis: Sei R ein Euklidischer Ring, $(0) \neq I \trianglelefteq R$. Sei $b \in I \setminus \{0\}$ von minimalem Rang unter den Elementen von $I \setminus \{0\}$ ($\rho(b) = \min\{\rho(a) \mid a \in I \setminus \{0\}\}$; das Minimum existiert, weil jede nichtleere Teilmenge von $\mathbb{N}_0$ ein Minimum hat). Wir zeigen: $I = (b)$.

Für beliebiges $a \in I$: Division mit Rest durch b. $a = qb + r$ und $r = 0$ oder $\rho(r) < \rho(b)$. Da $r = a - qb$ und $a, b \in I$, folgt $r \in I$, also kann $\rho(r) < \rho(b)$ nicht gelten. Es folgt $r = 0$ und $a = qb \in (b)$. Also gilt $I \subseteq (b) \subseteq I \Rightarrow I = (b)$. ∎

Übungsbeispiele

Übung 15: Seien $n \in \mathbb{N}, k \in \mathbb{Z}$ mit $\mathrm{ggT}(n, k) = 1$. Zeigen Sie, dass man mit dem Euklidischen Algorithmus ein Inverses zu $k + n\mathbb{Z}$ in $\mathbb{Z}_n$ finden kann.

Übung 16: Seien $n, m \in \mathbb{N}$. Dann ist

$$f : \mathbb{Z}_n \to \mathbb{Z}_{mn} \quad f(k) = mk$$

ein injektiver Gruppenhomomorphismus der additiven Gruppen, aber, wenn nicht $m \equiv 1$ mod n, kein Ringhomomorphismus. (In der Definition von f steht der Repräsentant für die entsprechende Klasse.)

Übung 17: Sei R ein Euklidischer Ring, dessen Rangfunktion $\rho(ab) \geq \rho(a)$ (für $a, b \in R$ mit $ab \neq 0$) erfüllt. Zeigen Sie: $u \in R$ ist Einheit genau dann, wenn u minimalen Rang hat (d.h., wenn $\rho(u) = \min\{\rho(a) \mid a \in R \setminus \{0\}\}$).

Übung 18: Zeigen Sie, dass $R = \mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ ein Euklidischer Ring ist mit der Rangfunktion $N(a + bi) = a^2 + b^2$ (für $a, b \in \mathbb{Z}$). (Hinweis: zuerst Division mir Rest von Elementen aus R durch Elemente aus $\mathbb{N}$ zeigen; dann Division von $r \in R$ durch $z \in R$ (wobei $z \neq 0$) via Divison von $r\bar{z}$ durch $z\bar{z}$ zeigen.)

Übung 19: Finden Sie mit Hilfe des Euklidischen Algorithmus $\alpha, \beta, \gamma \in \mathbb{Z}$ mit

$$\alpha \cdot 45 + \beta \cdot 63 + \gamma \cdot 35 = 1.$$

Übung 20: Wir definieren Primzahl als $p \in \mathbb{Z} \setminus \{0, 1, -1\}$, sodaß p in $\mathbb{Z}$ keine Teiler außer $1, -1, p, -p$ hat. Zeigen Sie, dass $\mathbb{Z}_n$ genau dann ein Körper ist, wenn n eine Primzahl ist.

Übung 21: Sei K ein Körper. Für jeden Teilraum V des n-dim K-Vektorraums K^n (geschieben als Zeilenvektoren) ist die Menge J_V aller Matrizen in $M_n(K)$, deren Zeilen in V liegen, ein Linksideal von $M_n(K)$. Zeigen Sie, dass alle Linksideale von $R = M_n(K)$ von dieser Form sind. Hinweis: gegeben Linksideal J, sei V der von allen Zeilen aller Matrizen in J erzeugte Vektorraum. Matrizen in J_V lassen sich aus Matrizen in J durch Multiplikation von links mit bestimmten Matrizen in $M_n(K)$ und Addition schrittweise erzeugen (z.B. zuerst nur Matrizen konstruieren, deren erste Zeile beliebig in V ist, restliche Zeilen Null).

Übung 22: Sei R ein kommutativer Ring mit 1, $a, b \in R$. Wenn ein ggT u von a, b existiert, der eine Einheit ist, dann ist jede Einheit von R ein ggT von a, b, und jeder gemeinsame Teiler von a, b ist eine Einheit.

Bemerkung: wir schreiben im Folgenden $\mathrm{ggT}(a, b) = 1$ für die Tatsache, dass 1 ein ggT von a, b ist (und demnach alle gemeinsamen Teiler von a, b genau die Einheiten von R sind). Weiters schreiben wir $\mathrm{ggT}(a, b) = d$ für die Tatsache, dass a, b den gemeinsamen Teiler d haben, auch wenn d nicht eindeutig bestimmt ist (sondern nach Bsp. 14 nur bis auf die Äquivalenzrelation gegenseitigen Teilens). In einem Integritätsbereich folgt aus $\mathrm{ggT}(a, b) = d$, dass genau die Ringelemente der Form du, u eine Einheit von R, die verschiedenen ggT von a, b sind.

Übung 23: Sei R ein Integritätsbereich, $a, b \in R$. Wenn d ein ggT von a, b und $a = da'$, $b = db'$, dann gilt $\mathrm{ggT}(a', b') = 1$.

6 Polynomring

Definition 6.1 Sei R ein Ring (mit 1). Der *Polynomring* in einer Unbestimmten über R ist definiert als

$$\{(a_n)_{n\in\mathbb{N}_0} \mid a_i \in R;\ \text{nur endlich viele } a_i \neq 0\}$$

mit koordinatenweiser Addition:

$$(a_i)_{i\in\mathbb{N}_0} + (b_i)_{i\in\mathbb{N}_0} = (a_i + b_i)_{i\in\mathbb{N}_0}$$

und folgender Multiplikation (*Faltung*):

$$(a_n)_{n\in\mathbb{N}_0} \cdot (b_n)_{n\in\mathbb{N}_0} = (c_n)_{n\in\mathbb{N}_0}, \text{ wobei } c_n = \sum_{k=0}^{n} a_k b_{n-k} = \sum_{\substack{k,l\,\in\,\mathbb{N}_0 \\ k+l=n}} a_k b_l.$$

Bemerkung: Die Ringaxiome sind erfüllt.

Bemerkung: Die additive Gruppe ist direkte Summe von Kopien von $(R,+)$ indiziert mit $\mathbb{N}_0$: $\sum_{n\in\mathbb{N}_0} R$.

Assoziativität der Multiplikation: Sowohl $((a_n)(b_n))(c_n)$, als auch $(a_n)((b_n)(c_n))$ haben als n-te Koordinate: $\sum\limits_{\substack{k,l,m\,\in\,\mathbb{N}_0 \\ k+l+m=n}} a_k b_l c_m$.

Bemerkung: Ein Ringmonomorphismus: $R \to$ Polynomring ist durch $r \mapsto (r,0,0,\ldots)$ gegeben. Es ist daher eine „isomorphe Kopie“ von R eingebettet im Polynomring in Form der konstanten Polynome: $(a_0,a_1,\ldots)$ ist *konstantes* Polynom, wenn $\forall i > 0 :\ a_i = 0$.

Schreibweise mit „x “:

$x := (0,1,0,0,\ldots)$ $\quad (= e_1$, der erste Einheitsvektor). Man bezeichnet den Polynomring dann mit $R[x]$.

Nach Definition der Multiplikation ist $x^2 = x \cdot x = (0,0,1,0,0,\ldots)$, bzw. allgemein:

$x^k = (0,\ldots,0,1,0,0,\ldots)$, wobei die 1 an k-ter Stelle steht.

$x^0 = (1,0,0,\ldots) = e_0$, das Einselement im Polynomring.

Multiplikation mit konstanten Polynomen:

$$(r,0,0,\ldots)\cdot(a_0,a_1,\ldots) = (ra_0, ra_1,\ldots).$$

Jedes Element im Polynomring hat dann eine eindeutige Darstellung der Form

$$(a_n)_{n\in\mathbb{N}_0} = \sum_{n=0}^{N} r_n x^n.$$

Sei nämlich N so, dass $a_n = 0$ für $n > N$ ist, dann gilt

$$(a_n)_{n\in\mathbb{N}_0} = (a_0, \ldots, a_n, 0, 0, \ldots) = a_0 1 + a_2 x + \ldots + a_n x^n$$

Die $r_i = a_i$ sind eindeutig bestimmt, bis auf Hinzufügen von beliebig vielen $a_i = 0$ für $i > N$.

Definition 6.2 (Grad eines Polynoms) Sei $f = (a_n)_{n\in\mathbb{N}_0} = \sum a_n x^n \in R[x]$.

- Wenn $f = 0$, d.h. $\forall n\ a_n = 0$, dann sei $\deg f := -\infty$.
- Wenn $f \neq 0$, dann sei $\deg f := \max\{n \in \mathbb{N} \mid a_n \neq 0\}$.

Wenn $f \neq 0$ und $m = \max\{n \in \mathbb{N} \mid a_n \neq 0\}$, dann heißt a_m der *Leitkoeffizient* von f (das Nullpolynom hat keinen Leitkoeffizienten).

Bemerkung: Da wir $r \in R$ mit $(r, 0, 0, \ldots) = r + 0x + 0x^2 + \ldots$ identifizieren, d.h. $R \simeq \{(r, 0, 0, \ldots) \mid r \in R\} \leq R[x]$, gilt für $f = (a_n)_{n\in\mathbb{N}_0} \in R[x]$:

$$\begin{aligned} f = (a_n)_{n\in\mathbb{N}_0} \in R &\iff \forall n > 0\ a_n = 0 \\ &\iff \deg f = 0 \vee \deg f = -\infty \\ &\iff \deg f \leq 0 \end{aligned}$$

Proposition 6.3 (Rechenregeln für den Grad) Sei R ein Ring, $f, g \in R[x]$. Dann gilt:

1. $\deg(f + g) \leq \max(\deg f, \deg g)$
2. $\deg f \neq \deg g \ \Rightarrow\ \deg(f + g) = \max(\deg f, \deg g)$
3. $\deg(fg) \leq \deg f + \deg g$
4. Wenn f oder g einen Leitkoeffizienten hat, der kein Nullteiler ist, dann gilt sogar $\deg(fg) = \deg f + \deg g$.
5. R nullteilerfrei $\Rightarrow \deg(fg) = \deg f + \deg g$.

Beweis: zu 3., 4.: Sei $f = \sum a_n x^n$, $g = \sum b_n x^n$, $\deg f = n, \deg g = m$. In $f \cdot g = \sum c_i x^i$ sind alle c_i mit $i > n + m$ jedenfalls 0. $c_{n+m} = a_n b_m$ und $a_n \neq 0$, $b_m \neq 0$. In einem Ring mit Nullteilern könnte $a_n b_m$ trotzdem 0 sein, daher $\deg(fg) \leq \deg f + \deg g$. ∎

Proposition 6.4 Sei K ein Körper, dann ist $K[x]$, der Polynomring in einer Unbestimmten über K ein Euklidischer Ring mit Rangfunktion deg. Das heißt, für alle f, $g \in K[x]$ mit $g \neq 0$ gibt es $q, r \in K[X]$, sodass $f = qg + r$ und $r = 0$ oder $\deg r < \deg g$.

BEMERKUNG: Mit der Konvention $\deg 0 = -\infty$ kann man den Fall $r = 0$ auch unter $\deg r < \deg g$ subsummieren und erhält

$$\forall f, g \text{ mit } g \neq 0 \; \exists q, r : \; f = qg + r \text{ und } \deg r < \deg g.$$

BEMERKUNG: Wenn R ein Ring und kein Körper ist, dann ist $R[x]$ im Allgemeinen kein Euklidischer Ring, aber man kann durch Polynome, deren Leitkoeffizient eine Einheit ist, dividieren. Allgemeiner:

$$f = \sum a_n x^n; g = \sum b_n x^n; b_m \text{ der Leitkoeffizient von g}$$

Wenn $\forall n : b_m \mid a_n$ und $b_m \mid b_n$, dann

$$\exists q, r \in R[x] : \; f = qg + r \text{ und } \deg r < \deg g.$$

BEMERKUNG: Wenn K ein Körper ist, dann ist $K[x]$ ein Euklidischer Ring, also insbesondere ist $K[x]$ ein Hauptidealring. Aber z.B. $\mathbb{Z}[x]$ ist kein Hauptidealring: $(2, x)$, das von 2 und x erzeugte Ideal ist kein Hauptideal.

Definition 6.5 (Polynomring in mehreren Unbestimmten) Elemente des *Polynomrings in mehreren Unbestimmten* sind Folgen indiziert mit $(\mathbb{N}_0)^n = \mathbb{N}_0 \times \ldots \times \mathbb{N}_0$, in denen nur endlich viele Einträge ungleich 0 sind.

$$R[x_1, \ldots x_n] := \{(a_k)_{k \in \mathbb{N}_0^n} \mid \forall k = (k_1, \ldots, k_n) \in N_0^n : \; a_k \in R; \text{ nur endlich viele } a_k \neq 0\}$$

mit koordinatenweiser Addition:

$$(a_k)_{k \in \mathbb{N}_0^n} + (b_k)_{k \in \mathbb{N}_0^n} = (a_k + b_k)_{k \in \mathbb{N}_0^n}$$

und der Multiplikation (*Faltung*):

$$(a_k)_{k \in \mathbb{N}_0^n} \cdot (b_k)_{k \in \mathbb{N}_0^n} = (c_k)_{k \in \mathbb{N}_0^n}, \text{ wobei } c_k = \sum_{\substack{l, m \in \mathbb{N}_0^n \\ l + m = k}} a_l b_m \text{ mit } l + m := (l_1 + m_1, \ldots, l_n + m_n).$$

Man definiert $x_i := (a_k)_{k \in \mathbb{N}_0^n}$, wobei $a_k = 1$ für $k = (0, \ldots, 0, 1, 0, \ldots, 0) = e_i$ und $a_k = 0$ für $k \neq e_i$.

BEMERKUNG: Man stellt fest, dass x^k genau beim Index $(0, \ldots, 0, k, 0, \ldots)$ einen Koeffizienten $\neq 0$, nämlich 1 hat, und dass $x_1^{k_1} \cdot \ldots \cdot x_n^{k_n}$ genau an der Stelle (Index) $k = (k_1, \ldots, k_n)$ eine Eintragung $\neq 0$, nämlich 1, hat. Daher lässt sich jedes Polynom schreiben als

$$(a_k)_{k \in \mathbb{N}_0^n} = \sum_{k = (k_1, \ldots, k_n) \in \mathbb{N}_0^n} a_k x_1^{k_1} \ldots x_n^{k_n}$$

(endliche Summe, da nur endlich viele $a_k \neq 0$).

Multiindexschreibweise: Man schreibt x^k für $x_1^{k_1} \ldots x_n^{k_n}$ $(k = (k_1, \ldots, k_n))$, bzw. $a_k x^k$ für $a_{(k_1, \ldots, k_n)} x_1^{k_1} \ldots x_n^{k_n}$.

BEMERKUNG: Es existiert ein natürlicher Ringisomorphismus:

$$R[x,y] \simeq (R[x])[y] \simeq (R[y])[x].$$

Allgemeiner:

$$R[x_1,\ldots,x_n] \simeq R[x_1]\ldots[x_n]$$

BEMERKUNG: $R[x_1,\ldots,x_n]$ heißt *Polynomring in n Unbestimmten über R*, wobei $e_{(0,\ldots,0,1,0,\ldots,0)}$ (1 an i-ter Stelle) mit x_i abgekürzt wird.
$(a_{e_i} = 1, a_k = 0 \text{ für } k \neq e_i : (a_k)_{k\in\mathbb{N}_0^n} = e_{(0,\ldots,0,1,0,\ldots,0)})$

BEISPIEL: für einen Ring, der kein Hauptidealring ist: K sei ein Körper. Das Ideal (x,y) von $K[x,y]$ (das von $\{x,y\}$ erzeugte Ideal) lässt sich nicht von einem Element erzeugen.

In $K[x,y]$ existiert ein $\mathrm{ggT}(x,y)$, nämlich $\mathrm{ggT}(x,y) = 1$ (Ein Polynom, das x und y teilt, ist eine Konstante $\neq 0$, also eine Einheit). Aber es gibt keine $f,g \in K[x,y]$, sodass

$$f(x,y)x + g(x,y)y = 1.$$

Der ggT lässt sich also nicht als $K[x,y]$-Linearkombination darstellen.

Definition 6.6 Ein *Bézout-Ring* ist ein Ring, in dem jedes endlich erzeugte Ideal ein Hauptideal ist, d.h.

$$\forall a_1,\ldots,a_n \in R\ \exists d \in R:\ (a_1,\ldots,a_n) = (d).$$

Ein kommutativer Ring mit 1 ist also Bézout, wenn

$$\forall a_1,\ldots,a_n \in R\ \exists d \in R:\ a_1R + \ldots + a_nR = dR.$$

BEMERKUNG: Wir formulieren die Definition des ggT als Aussage über Hauptideale:
$d = \mathrm{ggT}(a,b)$, wenn

1. $d \mid a$, $d \mid b$
2. $\forall c$ mit $c \mid a$ und $c \mid b$: $c \mid d$

Das ist äquivalent zu:

1. $(a) \subseteq (d)$ und $(b) \subseteq (d)$
2. $\forall c$ mit $(a) \subseteq (c)$ und $(b) \subseteq (c)$: $(d) \subseteq (c)$

Das heißt, $d = \mathrm{ggT}(a,b)$ genau dann, wenn (d) das minimale Hauptideal ist, das (a) und (b) enthält, in dem Sinne, dass jedes Hauptideal (c), das (a) und (b) enthält, auch (d) enthält.

Proposition 6.7 Für einen kommutativen Ring R mit 1 ist äquivalent:

1. R Bézout
2. $\forall a, b \in R\ \exists d = \mathrm{ggT}(a, b)$ und $\exists \alpha, \beta \in R:\ d = \alpha a + \beta b$.

Beweis: ($\Rightarrow$) Wenn $(a, b) = (d)$, dann ist (d) das minimale Hauptideal, das $(a), (b)$ enthält, also ist $d = \mathrm{ggT}(a, b)$. Da $d \in dR = aR + bR$, lässt sich d als $\alpha a + \beta b$ schreiben.

($\Leftarrow$) $d = \alpha a + \beta b \Rightarrow d \in (a, b)$, also $(d) \subseteq (a, b)$. Andererseits gilt

$$d = \mathrm{ggT}(a, b) \Rightarrow (a) \subseteq (d), (b) \subseteq (d),$$

also $(a, b) \subseteq (d)$. Insgesamt $(a, b) = (d)$.

Mit Induktion folgt für $a_1, \ldots, a_n$, dass $\exists d \in R : (d) = (a_1, \ldots, a_n)$. ∎

Übungsbeispiele

Übung 24: Sei R kommutativer Ring, $f, g \in R[x]$, $g \neq 0$, $\deg(g) = n$ und $a_n \in R$ der Koeffizient von x^n in g (der Leitkoeffizient von g). Zeigen Sie unter der Voraussetzung, dass a_n in R jeden Koeffizienten von f und g teilt, dass es $q, r \in R[x]$ gibt mit $f = qg + r$ und entweder $r = 0$ oder $\deg(r) < \deg(g)$.

Übung 25: Sei $f = x^5 + 3x^4 + 4x^3 + 12x^2 + 3x + 9$ und $g = x^3 + 6x^2 + 13x + 12$. Finden Sie mit Hilfe des Euklidischen Algorithmus in $\mathbb{Q}[x]$ den ggT $d \in \mathbb{Q}[x]$ von f und g sowie $\alpha, \beta \in \mathbb{Q}[x]$ mit $\alpha f + \beta g = d$

7 Einsetzen in Polynome und Polynomfunktionen

Definition 7.1 Sei R ein Ring (eventuell nicht kommutativ), $f = \sum_{k=0}^{n} a_k x^k \in R[x], r \in R$.

Einsetzen von r in f links heißt $r \mapsto \sum_{k=0}^{n} r^k a_k =: f_{\text{li}}(r)$.

Einsetzen von r in f rechts heißt $r \mapsto \sum_{k=0}^{n} a_k r^k =: f_{\text{re}}(r)$.

Wenn r kommutativ ist, ergeben beide Arten des Einsetzens dasselbe $f(r)$. Die Funktion: $R \to R;\ r \mapsto f(r)$ heißt die von f induzierte *Polynomfunktion* $f : R \to R$.

Bemerkung: Wir bezeichnen im Allgemeinen die Polynomfunktion mit demselben Symbol, wie das Polynom. Das ist eine missbräuchliche Notation, da verschiedene Polynome dieselbe Funktion ergeben können. Aus der Polynomfunktion kann man im Allgemeinen nicht eindeutig das Polynom rekonstruieren.

Beispiel: Sei p prim. In $\mathbb{Z}_p[x]$ ergibt $x^p - x$ die Nullfunktion: $\mathbb{Z}_p \to \mathbb{Z}_p$. $x^p - x$ ist aber nicht das Nullpolynom, nicht einmal ein konstantes Polynom: $\deg x^p - x = p \geq 2 > 0$.

Es gilt $\forall a \in \mathbb{Z}_p :\ a^p - a = 0$, weil $0^p = 0$ und für $a \neq 0$ ist a eine Einheit. Die Einheitengruppe $(\mathbb{Z}_p^*, \cdot) = (\mathbb{Z}_p \setminus \{0\}, \cdot)$ hat $p-1$ Elemente und in jeder endlichen Gruppe G gilt: $\forall g \in G :\ g^{|G|} = 1$, insbesondere also für $a \in \mathbb{Z}_p \setminus \{0\} : a^{p-1} = 1$, daher $a^p = a$.

Beispiel: Es kann vorkommen, dass $f \in R[x]$ mehr als $\deg f$ Nullstellen hat. In $\mathbb{Z}_6[x]$ hat $x^2 + x$ vier Nullstellen: $0, 2, 3, 5$. $x^3 - x$ hat 6 Nullstellen.

Es kann auch für einen Ring R ohne Nullteiler vorkommen, dass $f \in R[x]$ mehr als $\deg f$ Nullstellen hat.

Definition 7.2 Seien i, j, k beliebige Symbole. Definiere eine Menge

$$\mathbb{H} := \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{Q}\}$$

Die Addition auf dieser Menge sei durch

$$(a + bi + cj + dk) + (a' + b'i + c'j + d'k) = (a + a') + (b + b')i + (c + c')j + (d + d')k$$

erklärt, die Multiplikation durch

$$i^2 = j^2 = k^2 = -1,\ ij = k,\ jk = i,\ ki = j,\ ji = -k,\ kj = -i,\ ik = -j$$

(wobei $-i = (-1)i$ sei). Zudem soll das Distributivgesetz gelten.

Dann bildet $(\mathbb{H}, +, \cdot)$ einen nichtkommutativen Schiefkörper, die sogenannten rationalen *Quaternionen* (analog definiert man auch die reellen Quaternionen).

BEISPIEL: In $\mathbb{H}[x]$ hat x^2+1 die Nullstellen $\pm i,\ \pm j,\ \pm k$.

BEISPIEL: Es kann vorkommen, dass für $f, g \in R[x]$ und $r \in R$, r Nullstelle von $(f \cdot g)$, aber weder Nullstelle von f, noch von g ist. Wenn R Nullteiler hat, ist das offensichtlich, aber auch in $\mathbb{H}[x]$:

Sei $f(x) = x + i$, $g(x) = x - i$. $(f \cdot g)(x) = x^2 + 1$. Z.B. k ist Nullstelle von x^2+1, aber keine Nullstelle von $x + i$ oder $x - i$.

BEISPIEL: Es kann vorkommen, dass $(f \cdot g)(r) \neq f(r) \cdot g(r)$:

$f = x + i$, $g = x - i$, $r = k$
$(f \cdot g)(k) = k^2 + 1 = 0$
$f(k) \cdot g(k) = (k + i)(k - i) = k^2 + ik - ki - i^2 = ik - ki = -2j \neq 0$

Satz 7.3 (Einsetzhomomorphismus) *Sei R ein kommutativer Ring, dann gilt*

$$\forall f, g \in R[x]\ \forall r \in R:\ (f \cdot g)(r) = f(r) \cdot g(r),$$

das heißt Einsetzen eines fixen $r \in R$ ergibt einen Ringhomomorphismus

$$\Phi_r : R[x] \to R,\ \Phi_r(f) = f(r).$$

Beweis: Ist ein Spezialfall des folgenden Satzes. ∎

Satz 7.4 *Seien R, S kommutative Ringe, $\Phi : R \to S$ ein Ringhomomorphismus und $s \in S$. Dann gibt es genau einen Ringhomomorphismus $\overline{\Phi} : R[X] \to S$ mit $\overline{\Phi}|_R = \Phi$ und $\overline{\Phi}(x) = s$, nämlich*

$$\overline{\Phi}(\sum_{k=0}^{n} a_k x^k) = \sum_{k=0}^{n} \Phi(a_k) s^k.$$

Insbesondere gilt für $R = S$, $\Phi = \mathrm{id}_R$: Einsetzen von $s \in R$ ist ein Ringhomomorphismus: $R[x] \to R$, $f \mapsto f(s)$.

Beweis: Wenn ein Ringhomomorphismus $\psi : R[x] \to S$ mit $\psi|_R = \Phi,\ \psi(x) = s$ existiert, dann muss er die im Satz angegebene Form haben (Eindeutigkeit):

$$\psi(a_0+a_1x+\ldots+a_nx^n) = \psi(a_0)+\psi(a_1)\psi(x)+\ldots+\psi(a_n)\psi(x)^n = \Phi(a_0)+\Phi(a_1)s+\ldots+\Phi(a_n)s^n$$

Zur Existenz: $\overline{\Phi}$ ist Ringhomomorphismus: Sei $f = \sum_{k=0}^{n} a_k x^k$, $g = \sum_{k=0}^{m} b_k x^k$.

$$\begin{aligned}
\overline{\Phi}(f \cdot g) &= \overline{\Phi}\Big(\sum_{k=0}^{m+n} \Big(\sum_{i=0}^{k} a_i b_{k-i}\Big) x^k\Big) = \\
&= \sum_{k=0}^{m+n} \Big(\sum_{i=0}^{k} \Phi(a_i)\Phi(b_{k-i})\Big) s^k = \quad (s \text{ kommutiert mit } \Phi(b_{k-i})) \\
&= \sum_{k=0}^{m+n} \sum_{i=0}^{k} \Phi(a_i) s^i \Phi(b_{k-i}) s^{k-i} = \\
&= \sum_{i,j} \Phi(a_i) s^i \Phi(b_j) s^j = \\
&= \Big(\sum_{i=0}^{n} \Phi(a_i) s^i\Big)\Big(\sum_{j=0}^{m} \Phi(b_j) s^j\Big) = \\
&= \overline{\Phi}(f) \cdot \overline{\Phi}(g)
\end{aligned}$$

Bemerkung: Damit $(f \cdot g)(s) = f(s) \cdot g(s)$ gilt, muss zumindest s mit allen $r \in R$ kommutieren.

Übungsbeispiele

Übung 26:

(i) In einem kommutativen Ring mit 1 ist ein Ideal I genau dann ganz R, wenn I eine Einheit enthält.

(ii) Ein kommutativer Ring R mit 1 ist genau dann ein Körper, wenn (0) und R die einzigen Ideale von R sind.

Übung 27: Sei $d \in \mathbb{N}$ quadratfrei (d.h., durch kein Quadrat einer Primzahl teilbar). Sei

$$R = \mathbb{Z}[\sqrt{-d}] = \{a + b\sqrt{-d} \mid a, b \in \mathbb{Z}\}.$$

(i) Die ‚Norm' $N\colon R \to \mathbb{Z}$, definiert durch $N(a + b\sqrt{-d}) = a^2 + db^2$ (für $a, b \in \mathbb{Z}$) ist multiplikativ: $N(rs) = N(r)N(s)$.

(ii) $r \in R$ ist eine Einheit in R genau dann, wenn $N(r)$ eine Einheit in $\mathbb{Z}$ ist. (Hinweis: ein Teiler einer Einheit ist auch eine Einheit.)

Übung 28: Geben Sie einen Isomorphismus an zwischen $M_n(R[x])$, dem Ring der $n \times n$ Matrizen mir Eintragungen im Polynomring $R[x]$, und $M_n(R)[x]$, dem Polynomring in einer Unbestimmten mit Koeffizienten in $M_n(R)$. (Hiebei ist R ein kommutativer Ring mit Eins.)

Übung 29: Seien f, g und h Polynome in $R[x]$ (R ein kommutativer Ring mit Eins), davon f ein normiertes Polynom (d.h. mit Leitkoeffizient 1) sodass $f \cdot g = h$. Sei S ein Unterring von R. Zeigen Sie: wenn f und $h \in S[x]$, dann auch $g \in S[x]$.

Übung 30: Sei D ein Integritätsbereich und kein Körper, dann ist $D[x]$ kein Hauptidealring. (Betrachten Sie das Ideal J jener Polynome, deren konstanter Term in einem fixen Ideal $I \neq D$ von D liegt. Angenommen, ein einziges Polynom f erzeugt J; Fallunterscheidung f konstant oder nicht.)

8 Nullstellen und Linearfaktoren von Polynomen

Satz 8.1 (Polynomdivision mit eindeutig bestimmtem Quotienten und Rest) *Sei R ein Ring mit 1, $f, g \in R[x]$ und der Leitkoeffizient von g sei eine Einheit in R. Dann gibt es eindeutig bestimmte $q, r \in R[x]$ mit $f = qg + r$ und* $\deg r < \deg g$.

Beweis: zuerst Existenz: Wenn $\deg f < \deg g$, dann $f = 0 \cdot g + f$.
Sei jetzt $\deg f \geq \deg g (\geq 0)$. Induktion nach $\deg f$:

$\deg f = 0 \Rightarrow \deg g = 0 \Rightarrow g$ konstant; Leitkoeffizient von g ist Einheit $\Rightarrow g$ Einheit $\in R$. $f = fg^{-1}g + 0$.

$\deg f = n > 0$. $f = \sum_{k=0}^{n} a_k x^k$, $g = \sum_{k=0}^{m} b_k x^k$, $m \leq n$, b_m Einheit. Setze

$$\tilde{f} = f - a_n b_m^{-1} x^{n-m} g,$$

dann gilt $\deg \tilde{f} < n$. Nach Induktionsvoraussetzung gibt es $\tilde{q}, \tilde{r}$, sodass $\tilde{f} = \tilde{q}g + \tilde{r}$ und $\deg \tilde{r} < \deg g$.

$$f = \tilde{f} + a_n b_m^{-1} x^{n-m} g = (\tilde{q} + a_n b_m^{-1} x^{n-m}) g + \tilde{r}$$

Wähle $q = \tilde{q} + a_n b_m^{-1} x^{n-m}$ und $r = \tilde{r}$.

zur Eindeutigkeit: Angenommen $f = qg + r = q_1 g + r_1$, $\deg r < \deg g, \deg r_1 < \deg g$. Dann folgt $r - r_1 = (q_1 - q)g$ und $\deg(r - r_1) \leq \max(\deg r, \deg r_1) < \deg g$. g hat als Leitkoeffizient eine Einheit (keinen Nullteiler), daher $\deg(q_1 - q)g = \deg(q_1 - q) + \deg g$. Wenn $\deg(q_1 - q) \geq 0$, dann folgt $\deg(q_1 - q)g \geq \deg g > \deg(r - r_1)$. Das ist unmöglich, also muss $\deg(q_1 - q) = -\infty$, somit $q_1 - q = 0$ und daher auch $r - r_1 = 0$. ∎

Satz 8.2 (Restsatz) *Sei R ein Ring mit 1. $f = \sum_{k=0}^{n} a_k x^k \in R[x]$, $c \in R$, $f(c) := \sum_{k=0}^{n} a_k c^k$ (Einsetzen rechts). Dann gibt es genau ein $q \in R[x]$, sodass*

$$f(x) = q(x) \cdot (x - c) + f(c).$$

Bemerkung: Man kann für einen nicht kommutativen Ring R nicht einfach sagen: Division mit Rest von f durch $(x-c)$. $f(x) = q(x) \cdot (x-c) + d$, $d \in R$ (weil $\deg d \leq \deg(x-c) = 1$). Es ist dann nicht automatisch $d = f(c)$, weil wir keinen Einsetzhomomorphismus haben.

Beweis (des Restsatzes):

$$\begin{aligned} f(x) - f(c) &= \sum_{k=0}^{n} a_k x^k - \sum_{k=0}^{n} a_k c^k = \sum_{k=0}^{n} a_k (x^k - c^k) \\ &= \sum_{k=0}^{n} a_k (x^{k-1} + x^{k-2} c + \ldots + c^{k-1})(x - c) = q(x)(x - c) \end{aligned}$$

Die Eindeutigkeit folgt aus der Eindeutigkeit von q und r bei Division mit Rest von f durch $(x - c)$. ∎

BEMERKUNG: Das funktioniert auch mit links Einsetzen und $f(x) = (x-c) \cdot q(x) + f(c)$.

Korollar 8.3 Sei R ein Ring mit 1, $f = \sum_{k=0}^{n} a_k x^k \in R[x]$, $c \in R$.

- c ist Rechts-Nullstelle von f (d.h. $\sum_{k=0}^{n} a_k c^k = 0$) $\iff \exists q \in R[x] : \ f(x) = q(x)(x-c)$
- c ist Links-Nullstelle von f (d.h. $\sum_{k=0}^{n} c^k a_k = 0$) $\iff \exists q \in R[x] : \ f(x) = (x-c)q(x)$

Beweis: Wenn $\exists q \in R[x] : \ f(x) = q(x)(x-c)$, dann gilt wegen des Restsatzes auch $\exists q' \in R[x] : \ f(x) = q'(x)(x-c) + f(c)$. Aufgrund der Eindeutigkeit der Division mit Rest folgt $q' = q$, $f(c) = 0$.

Die Umkehrung folgt direkt aus dem Restsatz. ∎

Definition 8.4 $\operatorname{Int}\mathbb{Z} := \{f \in \mathbb{Q}[x] \mid \forall z \in \mathbb{Z} : \ f(z) \in \mathbb{Z}\}$ heißt *Ring der ganzwertigen Polynome in einer Variablen.*

$\operatorname{Int}(\mathbb{Z}^n) := \{f \in \mathbb{Q}[x_1, \ldots, x_n] \mid \forall z_1, \ldots, z_n \in \mathbb{Z} : \ f(z_1, \ldots, z_n) \in \mathbb{Z}\}$ heißt *Ring der ganzwertigen Polynome in mehreren Variablen.*

BEMERKUNG: $\mathbb{Z}[x] \subsetneqq \operatorname{Int}\mathbb{Z} \subsetneqq Q[x]$

z.B.: $\frac{x^p - x}{p} \in \operatorname{Int}(\mathbb{Z}) \setminus \mathbb{Z}[x]$ für p prim.

$$\binom{x}{n} = \frac{x(x-1)(x-2)\ldots(x-n+1)}{n!} \in \operatorname{Int}\mathbb{Z}$$

BEISPIEL: (Ringelemente, die keinen ggT haben)

$R = \operatorname{Int}\mathbb{Z}$

$f = x(x-1) \qquad g = x(x+1)$

$x \mid f; \quad x \mid g$ in $\operatorname{Int}\mathbb{Z}$
$2 \mid f; \quad 2 \mid g$ in $\operatorname{Int}\mathbb{Z}$

$$f = 2\frac{x(x-1)}{2} \qquad g = 2\frac{x(x+1)}{2}$$

Wenn f und g einen ggT d hätten, dann $2 \mid d$ und $x \mid d$. Ausserdem haben f und g in $\mathbb{Q}[x]$ keinen gemeinsamen Teiler c mit $\deg c \geq 2$, daher $\deg d = 1$. d ist ein Polynom vom Grad 1, das in $\mathbb{Q}[x]$ den Teiler x hat:

$$d = q \cdot x, \qquad q \in \mathbb{Q}$$

Gleichzeitig $2 \mid d$ in $\operatorname{Int}\mathbb{Z}$, also $q \cdot x = 2 \cdot h(x)$, $\deg h = 1$, h ganzwertig.

$$\frac{qx}{2} \text{ ganzwertig } \Rightarrow q \in 2\mathbb{Z}$$

Somit $d = 2kx$ für ein $k \in \mathbb{Z}$. Widerspruch, weil $2x$ kein Teiler von f, g in $\operatorname{Int}\mathbb{Z}$ ist:

$$f = x(x-1) = 2x \cdot \frac{x-1}{2} \text{ und } \frac{x-1}{2} \notin \operatorname{Int}\mathbb{Z}.$$

9 Irreduzible und prime Elemente - maximale Ideale und Primideale

Definition 9.1 Sei R ein kommutativer Ring mit Eins. $c \in R$ heißt *irreduzibel*, wenn $c \neq 0$ und c keine Einheit ist und $c = ab \;\Rightarrow\; (a \text{ Einheit } \vee\, b \text{ Einheit})$ gilt.

$p \in R$ heißt *prim*, wenn $p \neq 0$ und p keine Einheit ist und $p \,|\, ab \;\Rightarrow\; p \,|\, a \vee p \,|\, b$ erfüllt.

Proposition 9.2 Sei R ein kommutativer Ring mit 1, $p \in R$ prim und kein Nullteiler. Dann ist p irreduzibel.

Beweis: Es sei $p = ab$. Dann gilt insbesondere $p \,|\, ab$ und damit $p \,|\, a$ oder $p \,|\, b$, o.B.d.A. gelte ersteres. Dann ist $pd = a$ für ein $d \in R$, also $p = ab = pdb \;\Rightarrow\; p(1 - db) = 0$. Weil p kein Nullteiler ist, muss $1 - db = 0$, also $db = 1$ sein. Damit ist jedoch b eine Einheit.
Folglich ist p irreduzibel. ∎

Korollar 9.3 In einem Integritätsbereich ist jedes prime Element irreduzibel.

Beispiel: Im Allgemeinen müssen irreduzible Elemente nicht prim sein: In $\operatorname{Int}\mathbb{Z}$ sind 2 und x jeweils irreduzibel, jedoch nicht prim.

- 2 ist irreduzibel: $2 = ab$ in $\mathbb{Q}[x]$, dann sind $a, b \in \mathbb{Q}$. $\mathbb{Q} \cap \operatorname{Int}\mathbb{Z} = \mathbb{Z}$, also $a, b \in \mathbb{Z}$. $2 = ab \Rightarrow a \in \{\pm 1\}$ oder $b \in \{\pm 1\}$.
- x ist irreduzibel: $x = ab$ in $\mathbb{Q}[x]$, dann (o.B.d.A, da $1 = \deg x = \deg a + \deg b$) $a = \frac{c}{d}x$, $b = \frac{c'}{d'}$, mit $c, d, c', d' \in \mathbb{Z}$. Wie oben folgt $b \in \mathbb{Z}$ und $a = cx$ mit $c \in \mathbb{Z}$. Es folgt $x = ab = cbx \Rightarrow cb = 1$, also $b \in \{\pm 1\}$.
- 2 ist nicht prim: $2 \mid x(x-1)$, weil $x(x-1) = 2\frac{x(x-1)}{2}$, aber $2 \nmid x$, $2 \nmid (x-1)$, da $\frac{x}{2} \notin \operatorname{Int}\mathbb{Z}$ und $\frac{x-1}{2} \notin \operatorname{Int}\mathbb{Z}$.
- x ist nicht prim: $x \mid x(x-1) = 2\frac{x(x-1)}{2}$, aber $x \nmid 2$ und $x \nmid \frac{x(x-1)}{2}$, weil $\frac{x-1}{2} \notin \operatorname{Int}\mathbb{Z}$.

Definition 9.4 Sei R ein Ring und $P \trianglelefteq R$. P heißt *Primideal*, wenn $P \neq R$ und $\forall A, B \trianglelefteq R$ gilt: $AB \subseteq P \;\Rightarrow\; A \subseteq P \vee B \subseteq P$.

Definition 9.5 Sei R ein Ring und $(c) \neq R$ ein Hauptideal von R. Man sagt (c) ist *maximal unter den echten Hauptidealen* von R, wenn es kein Hauptideal $(d) \neq R$ von R gibt, das (c) echt umfasst. (d.h. $(c) \subsetneqq (d) \Rightarrow (d) = R$).

Proposition 9.6 Sei R ein Integritätsbereich, $c, p \in R$.

- p prim $\iff$ (p) ist Primideal $\neq \{0\}$.

- c irreduzibel $\iff (c) \neq (0)$, $(c) \neq R$, (c) ist maximal unter den echten Hauptidealen.

Beweis: als Übung ∎

Bemerkung: Alles außer

$(c) \neq (0)$, $(c) \neq R$, (c) maximal unter den echten Hauptidealen $\Rightarrow c$ irreduzibel

gilt auch in beliebigen kommutativen Ringen mit 1.

Lemma 9.7 Sei R ein kommutativer Ring, P ein Ideal von R, dann gilt

$$P \text{ Primideal} \quad \iff \quad P \neq R \quad \wedge \quad \forall a, b \in R: \; ab \in P \Rightarrow a \in P \vee b \in P$$

Beweis: ($\Leftarrow$) gilt in beliebigen Ringen: Sei $AB \subseteq P$ und P erfülle die Bedingung aus dem Lemma. Angenommen $A \nsubseteq P$, zu zeigen ist $B \subseteq P$: Wähle $a_0 \in A \setminus P$, dann gilt $\forall b \in B: \; a_0 b \in AB \subseteq P$. $a_0 \notin P \Rightarrow b \in P$, also insgesamt $B \subseteq P$.

($\Rightarrow$) In kommutativen Ringen gilt $(ab) = (a)(b)$. Sei $ab \in P$, dann gilt $P \supseteq (ab) = (a)(b)$. Da P Primideal ist, folgt $(a) \subseteq P \; \vee \; (b) \subseteq P$, also insbesondere $a \in P$ oder $b \in P$. ∎

Definition 9.8 Sei R ein Ring, $M \trianglelefteq R$. M heißt *maximales Ideal*, wenn $M \neq R$ ist und für alle $I \trianglelefteq R$ mit $M \subsetneq I \subseteq R$ bereits $I = R$ gelten muss (d.h. M ist in der Menge der Ideale $\neq R$, geordnet durch $\subseteq$, ein maximales Element).

Proposition 9.9 R sei ein Ring mit Eins und $M \trianglelefteq R$. Wenn M ein maximales Ideal ist, dann ist M auch ein Primideal.

Beweis: Sei M ein maximales Ideal, $A, B \trianglelefteq R$ und $AB \subseteq M$. Angenommen, $A \nsubseteq M$. Dann ist $A + M$ ein Ideal mit $M \subsetneq A + M$, also $A + M = R$, da M maximal ist. R ist ein Ring mit Eins, also folgt $B \trianglelefteq R \;\Rightarrow\; RB = B$. Damit ist

$$B = RB = (A + M)B = AB + MB \subseteq AB + M \subseteq M$$

(da $AB \subseteq M$). ∎

Beispiel: für Primideale, die nicht maximal sind: $(0) \trianglelefteq \mathbb{Z}$, $(x) \trianglelefteq K[x, y]$, $(x) \trianglelefteq \mathbb{Z}[x]$

Proposition 9.10 Sei R ein kommutativer Ring mit Eins und $P \trianglelefteq R$. Dann gilt

$$P \text{ ist Primideal} \iff {}^{R}\!/_{P} \text{ ist Integritätsbereich}$$

Beweis: Es gilt $P \neq R \iff {}^{R}\!/_{P} \neq \{0\}$, also bleibt zu zeigen

$$(ab \in P \Rightarrow a \in P \vee b \in P) \iff {}^{R}\!/_{P} \text{ nullteilerfrei.}$$

Da $a \in P \Leftrightarrow a + P = 0 + P$, ist

$$ab \in P \Rightarrow a \in P \vee b \in P$$

äquivalent zu

$$(a + P)(b + P) = 0 + P \Rightarrow a + P = 0 + P \quad \vee \quad b + P = 0 + P.$$

Proposition 9.11 Sei R ein kommutativer Ring mit Eins und $M \trianglelefteq R$. Dann gilt:

$$M \text{ ist maximales Ideal } \iff R/M \text{ ist Körper}$$

Beweis: Wir verwenden: S Körper $\iff (0), S$ sind die einzigen Ideale von S.

Nach dem 3. Isomorphiesatz sind die Ideale von ${}^{R}\!/_{M}$ genau von der Form ${}^{J}\!/_{M}$, wobei $J \trianglelefteq R$ mit $M \subseteq J$. Weiters gilt:

$${}^{\mathrm{J}}\!/_{\mathrm{M}} = {}^{\mathrm{R}}\!/_{\mathrm{M}} \Leftrightarrow J = R \text{ und } {}^{\mathrm{J}}\!/_{\mathrm{M}} = (0) \Leftrightarrow J = M.$$

Sei M ein maximales Ideal, dann gilt $M \subseteq J \trianglelefteq R \Rightarrow J = M \vee J = R$, also ist jedes Ideal von ${}^{R}\!/_{M}$ gleich (0) oder ${}^{R}\!/_{M}$. Somit ist ${}^{R}\!/_{M}$ ein Körper.

Sei umgekehrt ${}^{R}\!/_{M}$ ein Körper, dann besitzt ${}^{R}\!/_{M}$ nur die Ideale (0) und ${}^{R}\!/_{M}$. Somit besitzt R kein Ideal J mit $M \subsetneqq J \subsetneqq R$. Weiters gilt ${}^{R}\!/_{M} \neq \{0\}$, und daher $M \neq R$. Also ist M maximal. ∎

Bemerkung: Wenn R nicht kommutativ ist, dann gilt im Allgemeinen nicht

$$M \text{ maximal } \Rightarrow {}^{\mathrm{R}}\!/_{\mathrm{M}} \text{ Schiefkörper.}$$

Es gilt jedoch

$$M \text{ ist maximal unter den Links- und Rechtsidealen } \iff R/M \text{ ist Schiefkörper}$$

(d.h. für jedes Links- oder Rechtsideal J mit $M \subsetneqq J \subseteq R$ gilt bereits $J = R$)

Beispiel: In $M_n(K)$ sind (0) und $M_n(K)$ die einzigen beidseitigen Ideale. (0) ist also ein maximales Ideal, aber $M_n(K) = {}^{M_n(K)}\!/_{(0)}$ ist kein Schiefkörper.

Bemerkung: Für kommutative Ringe mit 1 kann man

M maximales Ideal $\Rightarrow M$ Primideal

auch so zeigen:

$$M \text{ maximal } \Rightarrow {}^{\mathrm{R}}\!/_{\mathrm{M}} \text{ Körper } \Rightarrow {}^{\mathrm{R}}\!/_{\mathrm{M}} \text{ Integritätsbereich } \Rightarrow M \text{ Primideal}$$

Definition 9.12 Der *Index* eines Ideals $I \trianglelefteq R$ ist

$$[R : I] := |\{r + I \mid r \in R\}| = \left| {}^{\mathrm{R}}\!/_{\mathrm{I}} \right|$$

(Der Index der Untergruppe $(I, +)$ von $(R, +)$.

Bemerkung: Sei R ein kommutativer Ring mit 1. Jedes Primideal P mit endlichem Index ist maximal: ${}^{R}\!/_{P}$ endlicher Integritätsbereich $\Rightarrow$ ${}^{R}\!/_{P}$ Körper.

Lemma von Zorn

Definition 9.13 Sei X eine Menge und $\leq \subseteq X \times X$ eine Relation (man schreibt $x \leq y$ für $(x, y) \in \leq$). $\leq$ heißt *Ordnungsrelation* (und $(X, \leq)$ heißt *geordnete* bzw. *halbgeordnete Menge*), wenn gilt:

1. $\forall x \in X \; x \leq x$
2. $\forall x, y, z \in X \; (x \leq y \wedge y \leq z) \; \Rightarrow \; x \leq z$
3. $\forall x, y \in X \; (x \leq y \wedge y \leq x \; \Rightarrow \; x = y)$

Definition 9.14 Sei $(X, \leq)$ eine geordnete Menge, $Y \subseteq X$.

- $s \in X$ heißt *obere Schranke* von Y, wenn $\forall y \in Y \; y \leq s$
- $y_0 \in Y$ heißt *maximales Element* von Y, wenn $\forall y \in Y \; (y_0 \leq y \; \Rightarrow y = y_0)$

Bemerkung: Eine obere Schranke von Y muss nicht unbedingt in Y liegen, ein maximales Element schon. Ein maximales Element y_0 ist im Allgemeinen keine obere Schranke (weil erlaubt ist, dass es in Y Elemente gibt, die mit y_0 nicht vergleichbar sind).

Definition 9.15 Eine geordnete Menge $(Y, \leq)$ heißt *totalgeordnet*, wenn

$$\forall x, y \in Y : (x \leq y \vee y \leq x).$$

Eine Teilmenge Y einer geordneten Menge $(X, \leq)$ heißt *Kette*, wenn Y bezüglich $\leq$ totalgeordnet ist, d.h. $\forall x, y \in Y \; (x \leq y \vee y \leq x)$.

Lemma 9.16 (Lemma von Zorn) Sei $(X, \leq)$ eine halbgeordnete Menge, $X \neq \emptyset$. Wenn jede Kette $Y \subseteq X$ eine obere Schranke in X hat, dann hat X ein maximales Element.

Bemerkung: Sei R ein Ring mit Eins und $I \trianglelefteq R$. Dann gilt $(I = R \; \Leftrightarrow \; 1 \in I)$.

Satz 9.17 *Sei R ein Ring mit Eins und $I \trianglelefteq R$. Wenn $I \neq R$, dann existiert ein maximales Ideal $M \trianglelefteq R$ mit $I \subseteq M$.*

Beweis: Sei $X = \{J \trianglelefteq R \,|\, I \subseteq J \subsetneq R\}$. Dann ist $X \neq \emptyset$, weil $I \in X$. X ist eine geordnete Menge durch $J \leq J' :\Leftrightarrow J \subseteq J'$. Jede Kette in X hat eine obere Schranke in X:
Sei $Y = \{J_\lambda \,|\, \lambda \in \Lambda\} \subseteq X$ eine Kette. Wenn $\Lambda = \emptyset$, dann ist jedes $x \in X$ eine obere Schranke. Sei andernfalls $J = \bigcup_{\lambda \in \Lambda} J_\lambda$. Dann gilt $\forall y = J_\mu \in Y$: $y \subseteq J$, also wäre J eine obere Schranke. Es bleibt jedoch zu zeigen, dass $J \in X$ ist:

- $0 \in J$, weil $0 \in J_\lambda$ für ein $\lambda \in \Lambda$. Daher ist $J \neq \emptyset$.
  Seien nun $a, b \in J$. Dann gibt es $\lambda, \mu \in \Lambda$ mit $a \in J_\lambda$ und $b \in J_\mu$. Weil Y eine Kette ist, muss $J_\lambda \subseteq J_\mu$ oder $J_\mu \subseteq J_\lambda$ gelten, o.B.d.A ersteres. Dann folgt $a, b \in J_\mu$, also $a - b \in J_\mu$ und folglich auch $a - b \in J$.
  Seien schließlich $a \in J$ und $r \in R$. Dann gibt es ein $\lambda \in \Lambda$ mit $a \in J_\lambda$. Weil J_λ ein Ideal ist, sind damit $ar, ra \in J_\lambda$ und somit auch $ar, ra \in J$.
  Folglich ist J ein Ideal.

- $I \subseteq J$ ist klar, weil für ein beliebiges $\lambda \in \Lambda$ $I \subseteq J_\lambda$ gilt.

- Da $\forall \lambda \in \Lambda$ $J_\lambda \neq R$ und folglich $1 \notin J_\lambda$ ist, muss $1 \notin J$ sein, und somit ist $J \neq R$.

Also ist J eine obere Schranke von Y, und man darf das Lemma von Zorn anwenden. Daher hat X ein maximales Element $M \in X$, d.h. $M \trianglelefteq R$, $I \subseteq M \subsetneq R$ und $\forall J \trianglelefteq R$ mit $I \subseteq J \subsetneq R$: wenn $M \subseteq J$, dann $J = M$. Also ist M ein maximales Ideal mit $I \subseteq M$. ∎

Übungsbeispiele

Übung 31: Sei R kommutativer Ring mit 1. $p \in R$ ist prim genau dann, wenn (p) ein Primideal ungleich (0) ist.

Übung 32: Sei R ein Integritätsbereich. $c \in R$ ist irreduzibel genau dann, wenn $(c) \neq (0)$, $(c) \neq R$ und für jedes $d \in R$ mit $(c) \subsetneq (d)$ gilt $(d) = R$.

Übung 33: Seien $S \subseteq R$ kommutative Ringe mit 1 und P ein Primideal von R. Dann ist $Q = P \cap S$ Primideal von S.

Übung 34: Sei K ein Körper, $K[x_1, \ldots, x_n]$ der Polynomring in n Unbestimmten über K, und $a_1, \ldots a_n \in K$. Zeigen Sie

(i) $\varphi\colon K[x_1, \ldots, x_n] \to K[x_1, \ldots, x_n]$ definiert durch $\varphi(f) = f(x_1 - a_1, \ldots, x_n - a_n)$ ist ein Automorphismus von $K[x_1, \ldots, x_n]$.

(ii) Das von $x_1 - a_1, \ldots, x_n - a_n$ erzeugte Ideal ist maximal. (Betrachten Sie zuerst das von $x_1, \ldots, x_n$ erzeugte Ideal.)

Übung 35: Sei K ein Körper, $K[x_1, \ldots, x_n]$ der Polynomring in n Unbestimmten über K. Sei $1 \leq k < n$. Das von $x_1, \ldots, x_k$ erzeugte Ideal von $K[x_1, \ldots, x_n]$ ist Primideal, aber nicht maximal; desgleichen das von $x_1 - a_1, \ldots, x_k - a_k$ erzeugte Ideal für beliebige $a_1, \ldots a_k \in K$.

10 Ringe mit eindeutiger Primfaktorenzerlegung, ZPE-Ringe

Definition 10.1 Ein Integritätsbereich R heißt *ZPE-Ring* oder *faktorieller Ring*, wenn

1. Für alle $a \in R$, $a \neq 0$, a keine Einheit, gibt es $n \in \mathbb{N}$ und irreduzible $c_1, \ldots, c_n \in R$, sodass $a = c_1 \cdot \ldots \cdot c_n$. D.h., jedes $a \neq 0$, das keine Einheit ist, hat eine Faktorisierung in irreduzible Elemente.
2. Wenn $c_1, \ldots, c_n$ und $d_1, \ldots, d_m$ irreduzibel sind und $c_1 \cdot \ldots \cdot c_n = d_1 \cdot \ldots \cdot d_m$ gilt, dann ist $n = m$ und es gibt eine Permutation $\pi \in S_n$, sodass $c_i \approx d_{\pi(i)}$ $(i = 1, \ldots, n)$. D.h., die Faktorisierung ist eindeutig bis auf die Reihenfolge und Assoziiertheit.

Bemerkung: $c \approx d$ heißt, es gibt eine Einheit u mit $c = du$.

Definition 10.2 Ein Integritätsbereich R heißt *atomar*, wenn $\forall a \in R$, $a \neq 0$, a keine Einheit $\exists n \in \mathbb{N}$, $c_1, \ldots, c_n$ irreduzibel: $a = c_1 \cdot \ldots \cdot c_n$.

Beispiel: $\operatorname{Int}\mathbb{Z}$ ist atomar, aber die Faktorisierung ist nicht eindeutig:

$$x(x-1)(x-1)\ldots(x-n+1) = n!\binom{x}{n}$$

$n!$ in $\mathbb{Z}$ in Primzahlen faktorisieren. (Diese sind auch in $\operatorname{Int}\mathbb{Z}$ irreduzibel.) Links stehen n irreduzible Faktoren, rechts (für grosses n) viel mehr.

Definition 10.3 Sei S eine Menge von Idealen in R. Man sagt, R erfüllt die *aufsteigende Kettenbedingung für Ideale in S*, wenn jede aufsteigende Kette

$$I_0 \subseteq I_1 \subseteq I_2 \subseteq \ldots$$

von Idealen in S nur endlich viele verschiedene Ideale enthält.

Lemma 10.4 Sei R ein Integritätsbereich. Wenn R die aufsteigende Kettenbedingung für Hauptideale erfüllt, dann hat jedes Element $a \neq 0$, keine Einheit, eine Faktorisierung in irreduzible Elemente.

Beweis: Sei

$$S = \{a \in R \mid a \neq 0,\ a \text{ keine Einheit},\ \nexists c_1, \ldots, c_n \text{ irreduzibel mit } a = c_1 \ldots c_n\}$$

Es ist zu zeigen, dass $S = \emptyset$. Angenommen, $a \in S$. Wenn $a = bc$, dann ist $b \in S$ oder $c \in S$ ($a \neq 0 \Rightarrow b, c \neq 0$; wären b, c Einheiten oder Produkte von Irreduziblen, dann auch a, also wäre $a \notin S$). Wegen $a \in S$ ist a insbesondere nicht irreduzibel, also existieren b, c (beide keine Einheiten), sodass $a = bc$ und $a \not\approx b$, $a \not\approx c$.
Damit können wir induktiv eine Folge $a = a_0, a_1, \ldots$ definieren, sodass $a_i \in S$, $a_{n+1} \mid a_n$, $a_{n+1} \not\approx a_n$. Es ergibt sich eine aufsteigende Hauptidealkette $(a_0) \subsetneq (a_1) \subsetneq \ldots$, im Widerspruch zur aufsteigenden Kettenbedingung für Hauptideale. Also gibt es für jedes $a \neq 0$, das keine Einheit ist, eine Darstellung der Form $a = c_1 \ldots c_n$ mit irreduziblen c_i. ∎

Satz 10.5 *Sei R ein Integritätsbereich. Dann ist R genau dann ein ZPE-Ring, wenn*

1′. *R erfüllt die aufsteigende Kettenbedingung für Hauptideale*

2′. *Jedes irreduzible Element von R ist prim*

Beweis:
$1' \Rightarrow 1$: siehe Lemma

$2' \Rightarrow 2$: Seien $c_1, \ldots, c_n, d_1, \ldots, d_m$ irreduzibel, sodass

$$c_1 \ldots c_n = d_1 \ldots d_m.$$

Wegen 2′ sind die c_i, d_i prim. Da c_1 prim ist, gibt es ein i, sodass $c_1 \mid d_i$. O.B.d.A. gelte $c_1 \mid d_1$. Da d_1 irreduzibel ist, folgt aus $d_1 = c_1 \cdot u_1$, dass u_1 eine Einheit ist (weil c_1 keine Einheit ist). Durch kürzen erhält man

$$c_2 \ldots c_n = (ud_2) \ldots d_m.$$

Mit Induktion nach $\max(n, m)$ zeigt man nun, dass $n = m$ und $c_i \approx d_i \forall i = 1, \ldots, n$.

$1, 2 \Rightarrow 1'$: Wir wissen $a \,|\, b \;\Leftrightarrow\; (b) \subseteq (a)$ und $a \approx b \;\Leftrightarrow\; (b) = (a)$ bzw. $(a \,|\, b \wedge a \not\approx b) \;\Leftrightarrow\; (b) \subsetneq (a)$. Eine aufsteigende Kette von Hauptidealen $(a_1) \subseteq (a_2) \subseteq \ldots$ entspricht daher einer absteigenden Teilerkette $a_1, a_2, \ldots$ (d.h. $\ldots \,|\, a_n \,|\, a_{n-1} \,|\, \ldots \,|\, a_2 \,|\, a_1$). Jedes a_i teilt a_1, aber a_1 hat nur endlich viele nichtassoziierte Teiler (bis auf Multiplikation mit Einheiten sind die Teiler von a_1 genau die Produkte einer Auswahl von $c_1, \ldots, c_n$, wenn $a_1 = c_1 \ldots c_n$ die eindeutige Darstellung von a_1 als Produkt irreduzibler Faktoren ist), also gibt es nur endlich viele verschiedene Hauptideale unter den (a_i).

$1, 2 \Rightarrow 2'$: Sei c irreduzibel und $c \mid ab$. Somit gibt es ein d, sodass $cd = ab$. Wir zerlegen in irreduzible Faktoren:

$$cd_1 \ldots d_n = a_1 \ldots a_m b_1 \ldots b_k$$

Wegen der Eindeutigkeit der Zerlegung gibt es ein i, sodass $c \approx a_i$, oder ein j, sodass $c \approx b_j$. O.B.d.A. $c \approx a_i$, also $c \mid a_i$, und da $a_i \mid a$, folgt $c \mid a$. ∎

Lemma 10.6 Jeder Hauptidealring erfüllt die aufsteigende Kettenbedingung für beliebige Ideale.

Beweis: Sei $I_0 \subseteq I_1 \subseteq I_2 \subseteq \ldots$ eine aufsteigende Kette von Idealen. Die Vereinigung einer Kette von Idealen ist wieder ein Ideal (prüfen!). Somit gilt $I = \bigcup_{k=0}^{\infty} I_k$ ist ein Ideal. Da R ein Hauptidealring ist, gibt es ein $r \in R$, sodass $I = (r)$. Es gibt $k \in \mathbb{N}$, sodass $r \in I_k$. Somit auch $r \in I_l$ für $l \geq k$. Also gilt für $l \geq k$:

$$I = (r) \subseteq I_l \subseteq \bigcup_{n=0}^{\infty} I_n = I$$

und daher $I_l = I$. ∎

Lemma 10.7 In einem Hauptidealring ist jedes irreduzible Element prim.

Beweis: Sei R ein Haupridealring und $c \in R$ irreduzibel. Es gilt $(c) \neq R$ und

$$\forall d : (c) \subsetneqq (d) \Rightarrow (d) = R.$$

Da in einem Hauptidealring jedes Ideal die Form (d) hat, ist (c) ein maximales Ideal, also auch ein Primideal. Somit ist c prim. ∎

Korollar 10.8 Jeder Hauptidealbereich ist ein ZPE-Ring.

Bemerkung: Hauptidealbereich heißt: Hauptidealring und Integritätsbereich.

Korollar 10.9 Jeder Euklidische Bereich ist ein ZPE-Ring. Insbesondere sind $\mathbb{Z}$ und $K[x]$ (für einen Körper K) ZPE-Ringe.

Definition 10.10 In einem ZPE-Ring R sei $\mathbb{P}$ ein Repräsentantensystem der Klassen bezüglich $\approx$, die aus primen Elementen bestehen.
(d.h. $\forall q \in R$, q prim, $\exists! p \in \mathbb{P}$ mit $p \approx q$)

Bemerkung: p prim, $q \mid p \wedge p \mid q \Rightarrow q$ prim.
Insbesondere also p prim, $p \approx q \Rightarrow q$ prim.

Beispiel: In $\mathbb{Z}$ ist jede Klasse bezüglich $\approx$ von primen Elementen der Form $\{-p, p\}$ für p Primzahl. Also wäre $\mathbb{P} = \{p \in \mathbb{Z} \mid p \text{ prim}, p > 0\}$ ein Repräsentantensystem.

Beispiel: In $K[x]$ (K Körper) sind die Einheiten genau die Konstanten $\neq 0$, also wäre

$$\mathbb{P} = \{f \in K[x] \mid f \text{ irreduzibel, normiert }\}$$

ein Repräsentantensystem der primen Elemente bezüglich $\approx$ (normiert bedeutet Leitkoeffizient $= 1$).

Proposition 10.11 (Primfaktorzerlegung) Sei R ein ZPE-Ring, $\mathbb{P}$ ein Repräsentantensystem der Assoziiertenklassen von primen Elementen von R. Dann hat jedes $a \neq 0$ eine eindeutige Darstellung in der Form

$$a = u_a \cdot \prod_{p \in \mathbb{P}} p^{v_p(a)}$$

wobei u_a Einheit ist, $v_p(a) \in \mathbb{N}_0$ und nur endlich viele $v_p(a) \neq 0$ sind.
Dabei ist $v_p(a)$ nur von der Assoziiertenklasse von p (und nicht von der Wahl des Repräsentantensystems $\mathbb{P}$) abhängig. D.h., wenn $\mathbb{P}'$ ein anderes Repräsentationsystem ist und $a = u'_a \cdot \prod_{p' \in \mathbb{P}'} p'^{v_{p'}(a)}$, dann gilt $p \approx p' \;\Rightarrow\; v_p(a) = v_{p'}(a)$.

Beweis: als Übung. ∎

BEMERKUNG: ZPE-Ring Eigenschaft für Hauptideale formuliert: Jedes Hauptideal $\neq (0)$ faktorisiert als $(r) = P_1 \dots P_n$, wobei die P_i prime Hauptideale sind. (Eindeutig bis auf Reihenfolge)

BEMERKUNG: Sei R ein ZPE-Ring, $r,\ s \in R \setminus \{0\}$ und $v_p(r)$ sei der Exponent, zu dem p in der Primfaktorzerlegung von R auftritt. Dann gilt

$$\forall p \in \mathbb{P} :\ v_p(rs) = v_p(r) + v_p(s).$$

Somit folgt auch für $a,\ b \in R \setminus \{0\}$:

$$a \mid b \iff \forall p \in \mathbb{P} :\ v_p(a) \leq v_p(b).$$

Daraus folgt für $a,\ b \in R \setminus \{0\}$:

$$\mathrm{ggT}(a,b) \approx \prod_{p \in \mathbb{P}} p^{\min(v_p(a), v_p(b))}$$
$$\mathrm{kgV}(a,b) \approx \prod_{p \in \mathbb{P}} p^{\max(v_p(a), v_p(b))}$$

Übungsbeispiele

Übung 36: Sei D ein Integritätsbereich. Dann sind die Einheiten in $D[x]$ genau die Konstanten, die in D Einheiten sind.

Übung 37: In einem ZPE-Ring haben je zwei Elemente $a, b \in R \setminus \{0\}$ einen ggT, nämlich

$$\mathrm{ggT}(a,b) = \prod_{p \in \mathbb{P}} p^{\min(v_p(a), v_p(b))}$$

und ein kgV, nämlich

$$\mathrm{kgV}(a,b) = \prod_{p \in \mathbb{P}} p^{\max(v_p(a), v_p(b))}.$$

Hinweis: $a \mid c \iff \forall p \in \mathbb{P}\ v_p(a) \leq v_p(c)$.

Übung 38: Für Elemente a, b, c eines ZPE-Ringes gilt: Wenn $a \mid bc$ und $\mathrm{ggT}(a,b) = 1$, dann $a \mid c$.

Übung 39: In Int$\mathbb{Z}$ gilt die Aussage von Bsp. 38 nicht. (Finden Sie konkrete $a, b, c \in$ Int$\mathbb{Z}$, die ein Gegenbeispiel darstellen.)

Übung 40: In einem kommutativen Ring mit 1 ist jede Nichteinheit in einem maximalen Ideal enthalten.

Übung 41: Ein kommutativer Ring mit 1 hat genau dann nur ein einziges maximales Ideal, wenn die Menge der Nichteinheiten ein Ideal ist.

Übung 42: In einem nichtkommutativen Ring mit 1 kann das von einer Nichteinheit erzeugte Ideal ganz R sein. Hinweis: in $R = M_2(K)$ die Matrix E_{12} mit der Eintragung 1 an der Stelle $(1, 2)$, sonst 0, betrachten.

11 Ring der Brüche

BEMERKUNG: Man erhält den Körper der rationalen Zahlen aus dem Ring der ganzen Zahlen durch $\mathbb{Q} := \{(a,b) \mid b \in \mathbb{Z} \setminus \{0\}\}/\sim$, wobei $\sim$ durch $(a,b) \sim (c,d) \ :\Leftrightarrow \ ad = bc$ definiert ist. Die Elemente von $\mathbb{Q}$ sind Äquivalenzklassen von Paaren bezüglich $\sim$, und man schreibt $\frac{a}{b}$ für die Klasse von (a,b). Die Addition ist durch $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$ gegeben, die Multiplikation durch $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$.
Diese Konstruktion wird im Folgenden verallgemeinert.

Definition 11.1 Sei S eine Teilmenge eines kommutativen Ringes R mit 1. S heißt *multiplikativ*, wenn $S \neq \emptyset$ und $s, t \in S \ \Rightarrow \ st \in S$ gilt.

BEISPIEL: Einige multiplikative Mengen:

1. Sei R ein kommutativer Ring. Dann ist S, definiert als Menge der Nicht-Nullteiler, multiplikativ: wenn a, b keine Nullteiler sind und $(ab)c = 0$, dann würde $a(bc) = 0$, also $bc = 0$ und damit $c = 0$ folgen. Also kann ab dann auch kein Nullteiler sein.
   Im Spezialfall, dass R ein Integritätsbereich ist, ist $S = R \setminus \{0\}$ multiplikativ.

2. Sei R ein kommutativer Ring, $P \trianglelefteq R$ ein Primideal und $S = R \setminus P$. Die Eigenschaft $ab \in P \ \Rightarrow \ a \in P \vee b \in P$ von P ist äquivalent zur Eigenschaft

   $$a \in S \wedge b \in S \ \Rightarrow \ ab \in S,$$

   und wegen $P \neq R$ ist $S \neq \emptyset$.

3. Sei P_i Primideal für $i \in I$. Dann ist $\bigcup_{i \in I} P_i$ multiplikativ.

4. $\{r^n \mid n \in \mathbb{N}_0\}$ ist für fixes $r \in R \setminus \{0\}$ multiplikativ, wenn r nicht nilpotent ist.

Definition 11.2 Eine multiplikative Menge S heißt gesättigt, wenn jeder Teiler eines $s \in S$ auch in S liegt, das heißt $\emptyset \neq S \subseteq R$ ist gesättigte multiplikative Menge genau dann, wenn

$$s \cdot t \in S \Longleftrightarrow s, t \in S.$$

Definition 11.3 Sei $S \subseteq R$ eine multiplikative Menge und

$$\overline{S} := \{t \in R \mid \exists r \in R : \ t \cdot r \in S\}.$$

$\overline{S}$ heißt *Sättigung* von S.

BEMERKUNG: $\overline{S}$ ist eine gesättigte multiplikative Menge.

Satz 11.4 (Ring der Brüche) *Sei R ein kommutativer Ring, $S \subseteq R$ multiplikativ.*

1. *Die auf $R \times S$ durch $(r,s) \sim (r',s') \;:\Leftrightarrow\; \exists t \in S$ mit $t(rs' - r's) = 0$ definierte Relation ist eine Äquivalenzrelation.*
   Wenn S keine Nullteiler enthält, dann hat die Relation die einfachere Form

$$(r,s) \sim (r',s') \;\Leftrightarrow\; rs' - r's = 0.$$

   Wir bezeichnen die Äquivalenzklasse von (r,s) bezüglich $\sim$ mit $\frac{r}{s}$ und die Menge der Äquivalenzklassen $(R \times S)/_\sim = \{\frac{r}{s} \mid r \in R, s \in S\}$ mit $S^{-1}R$ oder R_S.

2. *$S^{-1}R$ bildet bezüglich der Addition $\frac{r}{s} + \frac{r'}{s'} = \frac{rs'+r's}{ss'}$ und der Multiplikation $\frac{r}{s} \cdot \frac{r'}{s'} = \frac{rr'}{ss'}$ einen kommutativen Ring mit Eins, wobei $0_{S^{-1}R} = \frac{0}{s}$ und $1_{S^{-1}R} = \frac{s}{s}$ ($s \in S$ beliebig).*

Beweis:

1. als Übung.

2. - $+$ ist wohldefiniert: sei $\frac{r}{s} = \frac{\rho}{\sigma}$ und $\frac{r'}{s'} = \frac{\rho'}{\sigma'}$. Zu zeigen ist dann, dass $\frac{r}{s} + \frac{r'}{s'} = \frac{\rho}{\sigma} + \frac{\rho'}{\sigma'}$ gilt:
     Sei dazu $t \in S$ mit $t(r\sigma - \rho s) = 0$ und $t' \in S$ mit $t'(r'\sigma' - \rho' s') = 0$. Dann gilt:

$$\begin{aligned} tt'((rs' + r's)\sigma\sigma' - (\rho\sigma' + \rho'\sigma)ss') &= tt'(rs'\sigma\sigma' - r's\sigma\sigma' - \rho\sigma' ss' + \rho'\sigma ss') \\ &= t(r\sigma - \rho s)t's'\sigma' - t'(r'\sigma' - \rho' s')ts\sigma \\ &= 0t's'\sigma' - 0ts\sigma = 0 \end{aligned}$$

     Also ist $\frac{rs'+r's}{ss'} = \frac{\rho\sigma'+\rho'\sigma}{\sigma\sigma'}$.
   - Analog folgt, dass $\cdot$ wohldefiniert ist.
   - Assoziativität von $+$:

$$\left(\frac{r}{s} + \frac{r'}{s'}\right) + \frac{r''}{s''} = \frac{(rs' + r's)s'' + r''ss'}{ss's''} = \frac{rs's'' + r'ss'' + r''ss'}{ss's''}$$

$$\frac{r}{s} + \left(\frac{r'}{s'} + \frac{r''}{s''}\right) = \frac{rs's'' + (r's'' + r''s')s}{ss's''} = \frac{rs's'' + r'ss'' + r''ss'}{ss's''}$$

     Also sind die beiden Ausdrücke gleich.
   - Nullelement $\frac{0}{s}$: $\frac{r}{s} + \frac{0}{s} = \frac{rs+0s}{s^2} = \frac{rs}{s^2} = \frac{r}{s}$ (Kürzen ist nach dem vorigen Lemma möglich).
   - Die Operation $+$ ist kommutativ, weil R kommutativ ist.
   - Das Inverse von $\frac{r}{s}$ bezüglich $+$ ist $\frac{-r}{s}$: $\frac{r}{s} + \frac{-r}{s} = \frac{rs+(-r)s}{s^2} = \frac{0}{s^2} = 0_{S^{-1}R}$
   - Die Assoziativität von $\cdot$ ist klar. $\cdot$ ist überdies kommutativ, weil R kommutativ ist.

- Distributivgesetz:

$$\begin{aligned}\left(\frac{r}{s}+\frac{r'}{s'}\right)\frac{r''}{s''} & \\ &= \frac{(rs'+r's)r''}{ss's''} \\ &= \frac{rs'r''+r'sr''}{ss's''} \\ &= \frac{rr''s's''+r'r''ss''}{ss's''s''} \\ &= \frac{rr''}{ss''}+\frac{r'r''}{s's''}\end{aligned}$$

- Einselement $\frac{t}{t}$ (t beliebig): $\frac{r}{s}\cdot\frac{t}{t}=\frac{rt}{st}=\frac{r}{s}$ (kürzen).

Damit sind alle Eigenschaften eines kommutativen Ringes mit Eins gezeigt. ∎

Definition 11.5 $S^{-1}R$ heißt *Ring der Brüche von R mit Nennern in S*

Bemerkung: Wenn $0 \in S$, dann ist $S^{-1}R$ trivial, denn es besteht nur aus einem Element. $S^{-1}R = \{0\}$, weil für alle $\frac{r}{s}$, $\frac{r'}{s'}$ gilt $0rs = 0r's'$, also $\frac{r}{s} = \frac{r'}{s'}$.

Ab jetzt betrachten wir nur multiplikative Mengen S mit $0 \notin S$.

Falls $S = R \setminus P$ für ein Primideal P schreibt man R_P für R_S. (Es besteht keine Verwechslungsgefahr, da $0 \in P$, also kann P nicht die multiplikative Menge sein.)

Bemerkung: $\forall r \in R,\ s, t \in S:\ \frac{r}{s} = \frac{rt}{st}$.

Lemma 11.6 In R_S sind die Einheiten genau die $\frac{r}{t}$ mit $\exists t \in R:\ rt \in S$ und das Nullelement wird genau von den Brüchen $\frac{r}{s}$ dargestellt, für die $\exists t \in S:\ rt = 0$.

Beweis: Wenn $\frac{r}{s}$ Einheit, dann $\exists \frac{r'}{s'}$, sodass $\frac{r}{s}\frac{s'}{s'} = 1 = \frac{\sigma}{\sigma}$. Somit $\exists t \in S : trr'\sigma = tss'\sigma$. Somit gilt $(tr'\sigma)r = tss'\sigma \in S$.

Angenommen, $\exists t \in R:\ rt = \sigma \in S$. Wir wollen ziegen, dass $\frac{r}{s}$ eine Einheit ist. $\frac{rt}{s} = \frac{\sigma}{s}$ hat Inverses $\frac{s}{\sigma}$, also $\frac{rt}{s}\frac{s}{\sigma} = 1$. Daher $\frac{r}{s}\frac{ts}{\sigma} = 1$, also hat $\frac{r}{t}$ das Inverse $\frac{ts}{\sigma}$. ∎

Korollar 11.7 Sei S eine gesättigte multiplikative Menge, dann sind die Einheiten in R_S genau die $\frac{r}{s}$ mit $r \in S$. Das Nullelement wird durch jene Brüche $\frac{r}{s}$ dargestellt, für die r σ-Nullteiler eines $\sigma \in S$ ist (d.h. $\exists \sigma \in S:\ r\sigma = 0$).

Definition 11.8 Sei R ein Integritätsbereich, $S = R \setminus \{0\}$, dann ist R_S ein Körper, der *Quotientenkörper* von R.

BEMERKUNG: $R\backslash\{0\}$ ist genau dann multiplikative Menge, wenn R keine Nullteiler hat. R_S ist Körper, weil R_S ein kommutativer Ring mit 1 ist und jedes Element $\frac{r}{s} \neq 0$ invertierbar ist: $\frac{r}{s} \neq 0$ bedeutet insbesondere $r \neq 0$, somit $r \in R \setminus \{0\} = S$. Daher hat $\frac{r}{s}$ das Inverse $\frac{s}{r}$.

BEISPIEL: $\mathbb{Q}$ ist der Quotientenkörper von $\mathbb{Z}$.

Satz 11.9 *Sei S eine multiplikativ abgeschlossene Teilmenge eines kommutativen Ringes R, $0 \notin S$.*

1. *$\varphi_S : R \to S^{-1}R$, definiert durch $r \mapsto \frac{rs}{s}$ (dabei ist $s \in S$ beliebig) ist ein Ringhomomorphismus, und für alle $s \in S$ gilt: $\varphi_S(s)$ ist Einheit in $S^{-1}R$.*
2. *$\operatorname{Ker} \varphi_S = \{r \in R \mid \exists s \in S \text{ mit } rs = 0\}$*
3. *Wenn S keine Nullteiler enthält, dann ist φ_S injektiv.*

Beweis:

1. - φ_S ist wohldefniert: $s, t \in S$, $r \in R \Rightarrow \frac{rs}{s} = \frac{rt}{t}$, da $trs - srt = 0$.
   - $\varphi_S(r + r') = \frac{(r+r')s}{s} = \frac{rs+r's}{s} = \frac{rs^2+r's^2}{s^2} = \frac{rs}{s} + \frac{r's}{s} = \varphi_S(r) + \varphi_S(r')$
   - $\varphi_S(rr') = \frac{rr's}{s} = \frac{rr's^2}{s^2} = \frac{rs}{s} \cdot \frac{r's}{s} = \varphi_S(r) \cdot \varphi_S(r')$
   - Ist $s \in S$, dann ist $\varphi_S(s) = \frac{s^2}{s}$ Einheit mit dem Inversen $\frac{s}{s^2}$, wie zuvor gezeigt wurde.
2. Sei $\varphi_S(r) = 0_{S^{-1}R} = \frac{0}{s}$. Dann folgt $\frac{rs}{s} = \frac{0}{s}$, also $trs^2 - ts0 = 0$ für ein $t \in S$. Damit ist jedoch $r(ts^2) = 0$ und $ts^2 \in S$.
   Sei umgekehrt $rs = 0$ für ein $s \in S$. Dann ist $\varphi_S(r) = \frac{rs}{s} = \frac{0}{s} = 0_{S^{-1}R}$, also $r \in \operatorname{Ker} \varphi_S$.
3. Wenn S keine Nullteiler enthält, dann kann es für $r \in R$ nur dann ein $s \in S$ mit $rs = 0$ geben, wenn $r = 0$ ist. In diesem Fall ist dann $\operatorname{Ker} \varphi_S = \{0\}$, also φ_S injektiv.∎

BEMERKUNG: Wenn R ein Ring mit Eins ist und $1 \in S$, dann hat φ_S die einfache Form $\varphi_S(r) = \frac{r}{1}$.

BEMERKUNG: Sei R ein kommutativer Ring mit 1 und S die Menge der Nicht-Nullteiler von R. Dann heißt R_S der *komplette Ring der Brüche*. Das ist der „grösstmögliche“Ring der Brüche, in dem R injektiv eingebettet ist. (Sobald Nullteiler in S sind, ist $\varphi : R \to R_S$ nicht injektiv.)

Lemma 11.10 Seien R, T Ringe mit Eins, $g : R \to T$ ein Ringhomomorphismus.

1. Wenn ein Nicht-Nullteiler von T in $\operatorname{Im} g$ liegt, dann ist $g(1) = 1$.

2. Wenn $g(1) = 1$, dann gilt für jede Einheit $u \in R$: $g(u)^{-1} = g(u^{-1})$ (insbesondere ist dann $g(u)$ auch Einheit).

Beweis: als Übung. ∎

Satz 11.11 (Universelle Eigenschaft des Rings der Brüche) *Sei S eine multiplikativ abgeschlossene Teilmenge eines kommutativen Ringes R, $S^{-1}R = \{\frac{r}{s} \mid r \in R, s \in S\}$ der Ring der Brüche und $\varphi : R \to S^{-1}R$ durch $\varphi(r) = \frac{rs}{s}$ definiert.*
Wenn T ein kommutativer Ring mit Eins ist und $f : R \to T$ ein Ringhomomorphismus, sodass für alle $s \in S$ $f(s)$ eine Einheit in T ist, dann gibt es genau einen Ringhomomorphismus $\overline{f} : S^{-1}R \to T$ mit $\overline{f} \circ \varphi = f$. Wenn f injektiv ist, dann auch $\overline{f}$.

Beweis: Definiere $\overline{f}(\frac{r}{s}) = f(r)f(s)^{-1}$. Dann sind alle Bedingungen erfüllt:

- $\overline{f}$ ist wohldefiniert: sei $\frac{r}{s} = \frac{r'}{s'}$ und $t \in S$ mit $t(rs' - r's) = 0$. Dann ist

  $$0 = f(0) = f(t)(f(r)f(s') - f(r')f(s)) = f(t)f(s)f(s')(f(r)f(s)^{-1} - f(r')f(s')^{-1})$$

  Weil $f(t)f(s)f(s')$ Einheit und daher kein Nullteiler ist, muss somit

  $$f(r)f(s)^{-1} = f(r')f(s')^{-1}$$

  sein.

- $\overline{f}$ ist Homomorphismus bezüglich $+$:

  $$\begin{aligned}
  \overline{f}\left(\frac{r}{s} + \frac{r'}{s'}\right) &= \overline{f}\left(\frac{rs' + r's}{ss'}\right) \\
  &= f(rs' + r's)f(ss')^{-1} \\
  &= f(rs')f(ss')^{-1} + f(r's)f(ss')^{-1} \\
  &= \overline{f}\left(\frac{rs'}{ss'}\right) + \overline{f}\left(\frac{r's}{ss'}\right) \\
  &= \overline{f}\left(\frac{r}{s}\right) + \overline{f}\left(\frac{r'}{s'}\right)
  \end{aligned}$$

- $\overline{f}$ ist Homomorphismus bezüglich $\cdot$:

  $$\begin{aligned}
  \overline{f}\left(\frac{r}{s} \cdot \frac{r'}{s'}\right) &= \overline{f}\left(\frac{rr'}{ss'}\right) \\
  &= f(rr')f(ss')^{-1} \\
  &= f(r)f(s)^{-1}f(r')f(s')^{-1} \\
  &= \overline{f}\left(\frac{r}{s}\right) \cdot \overline{f}\left(\frac{r'}{s'}\right)
  \end{aligned}$$

- $\overline{f} \circ \varphi(r) = \overline{f}(\frac{rs}{s}) = f(rs)f(s)^{-1} = f(r)f(s)f(s)^{-1} = f(r)$, d.h. $\overline{f} \circ \varphi = f$.

Angenommen, g wäre ein anderer Ringhomomorphismus, der alle diese Bedingungen erfüllt. Für alle $s \in S$ ist $f(s)$ Einheit in T. $S \neq \emptyset$, daher gibt es ein $s \in S$, für das $f(s) = g(\varphi(s)) \in \operatorname{Im} g$ Einheit in T und damit kein Nullteiler ist. Nach dem vorigen Lemma gilt dann $g(1) = 1$, und für alle Einheiten $u \in S^{-1}R$ ist $g(u)$ Einheit mit $g(u)^{-1} = g(u^{-1})$. Damit ist jedoch

$$\begin{aligned} g\left(\frac{r}{s}\right) &= g\left(\frac{rs}{s}\frac{s}{s^2}\right) = g(\varphi(r)\varphi(s)^{-1}) = g(\varphi(r))g(\varphi(s)^{-1}) \\ &= g(\varphi(r))g(\varphi(s))^{-1} = f(r)f(s)^{-1} = \overline{f}\left(\frac{r}{s}\right) \end{aligned}$$

Also ist $\overline{f}$ eindeutig bestimmt.
Wenn f injektiv ist, dann ist $\operatorname{Ker} f = \{0\}$, also kann $0 = \overline{f}(\frac{r}{s}) = f(r)f(s)^{-1}$ nur dann gelten, wenn $f(r) = 0$, also $r = 0$ gilt. Damit ist jedoch $\operatorname{Ker} \overline{f} = \{0_{S^{-1}R}\}$, also $\overline{f}$ injektiv.∎

Korollar 11.12 Sein R ein Integritätsbereich und Q sein Quotientenkörper. Wenn $R \subseteq K$ für einen Körper K ist, dann gibt es eine isomorphe Kopie von Q mit $R \subseteq Q \subseteq K$, bestehend aus Elementen der Form rs^{-1} mit $r \in R$, $s \in R \setminus \{0\}$. ($f = \operatorname{incl}_{R \to K} : R \to K$, dann $\overline{f} : Q \to K$ mit $\overline{f}(\frac{r}{s}) = rs^{-1}$)

Definition 11.13 Sei K ein Körper. Der Quotientenkörper von $K[x]$ heißt *Körper der rationalen Funktionen*:

$$K(x) = \left\{ \frac{f(x)}{g(x)} \mid f, g \in K[x], g \neq 0 \right\}$$

Übungsbeispiele

Übung 43:

(i) In einem kommutativen Ring bilden die nilpotenten Elemente ein Ideal.

(ii) Die Nullteiler eines kommutativen Rings bilden im Allgemeinen kein Ideal. Geben Sie ein Gegenbeispiel an.

Übung 44: Sei I ein Ideal des kommutativen Rings R. Dann ist $I[x]$ (bestehend aus den Polynomen in $R[x]$, deren Koeffizienten in I liegen) ein Ideal von $R[x]$, und

$$\mathrm{R[x]}/\mathrm{I[x]} \simeq (\mathrm{R}/\mathrm{I})[x].$$

Übung 45: Sei R kommutativer Ring, $S \subseteq R$ eine multiplikative Menge und $\bar{S}$ deren Sättigung. Dann ist $f\colon R_S \to R_{\bar{S}}$, definiert durch $f(\frac{r}{s}) = \frac{r}{s}$ ein Ringisomorphismus.

Übung 46: Sei R kommutativer Ring, und für $i \in I$ (beliebige Indexmenge) P_i ein Primideal von R. Dann ist $S = R \setminus \bigcup_{i \in I} P_i$ eine gesättigte multiplikative Menge.

Übung 47: Die Nichtnullteiler eines kommutativen Rings bilden eine gesättigte multiplikative Menge.

12 Polynome über ZPE-Ringen

Definition 12.1 Sei R ein ZPE-Ring, $f(x) = \sum_{k=0}^{n} a_k x^k \in R[x]$, $f \neq 0$. Dann heißt $\mathrm{ggT}(a_0, \ldots, a_n)$ der *Inhalt* des Polynoms f. Wenn $\mathrm{ggT}(a_0, \ldots, a_n) \approx 1$, dann heißt f *primitives* Polynom. Man schreibt den Inhalt als $C(f)$.

Lemma 12.2 Sei R ein ZPE-Ring, $f \in R[x]$, $f \neq 0$, $a \in R$. Dann gilt:

1. $C(af) = aC(f)$
2. Zu f existiert ein primitives Polynom $\tilde{f}$ mit $f = C(f)\tilde{f}$.

Beweis: als Übung ∎

Bemerkung: Sei R ein ZPE-Ring mit Quotientenkörper Q, dann gilt

$$\forall 0 \neq f \in Q[x] \exists r \in Q : \; rf = \tilde{f}, \quad \tilde{f} \text{ primitiv } \in R[x].$$

Lemma 12.3 (Lemma von Gauß) Sei R ein ZPE-Ring, $f, g \in R[x]$ primitive Polynome. Dann ist fg primitiv.

Beweis: Es genügt zu zeigen, dass für jedes prime Element $p \in R$ ein Koeffizient c von fg existiert, sodass $p \nmid c$ (dann haben die Koeffizienten von fg keinen nichttrivialen gemeinsamen Teiler).
Sei also $p \in R$ prim, $f = \sum a_k x^k$, $g = \sum b_k x^k$, $fg = \sum c_k x^k$. Wähle n minimal, sodass $p \nmid a_n$ und m minimal, sodass $p \nmid b_m$ (existieren, weil f und g primitiv sind). Dann ist $c_{n+m} = \sum_{j+k=n+m} a_j b_k$. Für $j < n$ gilt aber $p \mid a_j$ und damit $p \mid a_j b_k$. Für $j > n$ ist andererseits $k < m$, daher $p \mid b_k$ und $p \mid a_j b_k$. Also ist $c_{n+m} \equiv a_n b_m \bmod p$, und weil p prim ist und weder a_n noch b_m teilt, teilt p auch $a_n b_m$ nicht, also $p \nmid c_{n+m}$. ∎

Korollar 12.4 Sei R ein ZPE-Ring, $f, g \in R[x]$, $f, g \neq 0$. Dann gilt $C(fg) = C(f)C(g)$.

Beweis: Es gilt $f = C(f)\tilde{f}$ und $g = C(g)\tilde{g}$ für primitive Polynome $\tilde{f}$ und $\tilde{g}$. Damit ist $C(fg) = C(C(f)\tilde{f}C(g)\tilde{g}) = C(f)C(g)C(\tilde{f}\tilde{g}) = C(f)C(g)$, da nach dem Lemma von Gauß $C(\tilde{f}\tilde{g}) = 1$ ist. ∎

Bemerkung: In allgemeinen kommutativen Ringen betrachtet man oft den

$$C(f) = (a_0, \ldots, a_n),$$

das von den Koeffizienten von f erzeugte Ideal von R.

Bemerkung: Seien $R \subseteq S$ Ringe, dann folgt aus der Irreduzibilität von $f \in S[x]$ in $S[x]$ nicht die Irreduzibilität von f in $R[x]$ und auch nicht umgekehrt.

Beispiel:

- $x^2 + 1$ ist irreduzibel in $\mathbb{R}[x]$, aber nicht in $\mathbb{C}[x]$
- $2x + 2$ ist irreduzibel in $\mathbb{Q}[x]$, aber nicht in $\mathbb{Z}[x]$

Lemma 12.5 Sei R ein Integritätsbereich, $c \in R$, dann gilt

$$c \text{ irreduzibel in } R[x] \iff c \text{ irreduzibel in } R.$$

Beweis: In $R[x]$ gilt $\deg(fg) = \deg f + \deg g$ (Integritätsbereich!). c ist konstant, das heißt $\deg c = 0$ oder $\deg c = -\infty$. Für alle f, g mit $fg = c$ gilt also $\deg f \leq 0$, $\deg g \leq 0$. Also gilt auch f, g konstant. ∎

Lemma 12.6 Sei R ein ZPE-Ring, Q sein Quotientenkörper, $f \in R[x]$, $f \neq 0$, und f primitiv. Dann gilt:

$$f \text{ irreduzibel in } R[x] \iff f \text{ irreduzibel in } Q[x]$$

Beweis: ($\Rightarrow$): Es sei f irreduzibel in $R[x]$. Angenommen, es gäbe $g, h \in Q[x]$, keine Einheiten, mit $f = gh$. Es gibt $c, d \in R$, sodass $cg \in R[x]$ und $dh \in R[x]$. Es folgt $cdf = (cg)(dh)$ in $R[x]$ und da f primitiv ist $C(cdf) = cd$. Insgesamt:

$$cd = C(cdf) = C(cg)C(dh)$$

Durch Herausheben des Inhalts erhält man $f = \tilde{g}\tilde{h}$, mit $\tilde{g}$, $\tilde{h}$ primitiv $\in R[x]$ und $cg = C(cg)\tilde{g}$, $dh = C(dh)\tilde{h}$.

Da g, h keine Einheiten in $Q[x]$ sind, sind sie insbesondere nicht konstant, somit sind auch $\tilde{g}$, $\tilde{h}$ nicht konstant, also keine Einheiten in $R[x]$. Somit gilt $g = \tilde{g}\tilde{h}$ in $R[x]$, und $\tilde{g}$, $\tilde{h}$ sind keine Einheiten, ein Widerspruch zur Irreduzibilität von f in $R[x]$.

($\Leftarrow$): Sei f irreduzibel in $Q[x]$. Angenommen, es gäbe $g, h \in R[x]$ mit $f = gh$. Dann muss g oder h Einheit in $Q[x]$ sein, o.B.d.A. sei g Einheit. Dann ist $g \in Q \setminus \{0\}$, $\deg g = 0$, und da auch $g \in R[x]$ ist, folgt $g \in R$. Aus $f = gh$ folgt $g \mid C(f)$ (g teilt jeden Koeffizienten von f). Somit gilt $g \mid 1$ in R und daher ist g eine Einheit in $R[x]$. ∎

Satz 12.7 *Ist R ein ZPE-Ring, dann ist auch $R[x]$ ZPE-Ring.*

Beweis:

- Existenz der Zerlegung in irreduzible Elemente:
  Wenn $c \in R \subseteq R[x]$ und $c = p_1 \dots p_m$, wobei die p_i irreduzibel in R sind, dann sind sie das auch in $R[x]$.
  Sei jetzt $\deg f \geq 1$. $f = C(f)\tilde{f}$, wobei $\tilde{f}$ primitiv ist. $C(f)$ lässt sich als Produkt irreduzibler Elemente schreiben, also genügt es zu zeigen, dass sich jedes primitive

Polynom $\tilde{f}$ als Produkt irreduzibler Elemente schreiben lässt.
Q sei der Quotientenkörper. Dann ist $Q[x]$ ein Euklidischer Bereich, also ein ZPE-Ring. Damit lässt sich $\tilde{f}$ als $\tilde{f} = h_1 \dots h_n$ mit irreduziblen $h_i \in Q[x]$ schreiben. Es gibt weiters $a_i \in R$ ($a_i \neq 0$), sodass $a_i h_i = g_i \in R[x]$ und primitive $\tilde{g_i} \in R[x]$ mit $g_i = C(g_i)\tilde{g_i}$. Dann ist $\tilde{g_i} = \frac{a_i}{C(g_i)} h_i$, und in $Q[x]$ gilt damit $\tilde{g_i} \approx h_i$, also ist $\tilde{g_i}$ irreduzibel in $Q[x]$, weil h_i irreduzibel in $Q[x]$ ist. Weil überdies $\tilde{g_i}$ primitiv ist, ist es auch irreduzibel in $R[x]$.
Es gilt $a_1 \dots a_n \tilde{f} = g_1 \dots g_n = C(g_1) \dots C(g_n) \tilde{g_1} \dots \tilde{g_n}$, und weil $\tilde{f}$ und $\tilde{g_1} \dots \tilde{g_n}$ primitiv in $R[x]$ sind, muss $a_1 \dots a_n \approx C(g_1) \dots C(g_n)$ in R gelten. Somit existiert eine Einheit $u \in R$ mit $C(g_1) \dots C(g_n) = u a_1 \dots a_n$. Damit ergibt sich

$$a_1 \dots a_n \tilde{f} = u a_1 \dots a_n \tilde{g_1} \dots \tilde{g_n},$$

also $\tilde{f} = (u\tilde{g_1})\tilde{g_2} \dots \tilde{g_n}$, d.h. $\tilde{f}$ hat eine Zerlegung in Irreduzible.

- Eindeutigkeit der Zerlegung in irreduzible Elemente:
Sei $f = p_1 \dots p_n g_1 \dots g_m$ mit konstanten irreduziblen $p_i \in R$ und irreduziblen Polynomen g_i mit $\deg g_i \geq 1$.
Weil g_i irreduzibel ist, ist es auch primitiv (sonst wäre $C(g_i)\tilde{g_i}$ eine nichttriviale Zerlegung). Also ist auch $g_1 \dots g_m$ primitiv.
Daher ist $C(f) \approx p_1 \dots p_n$. Wenn weiters $f = q_1 \dots q_k h_1 \dots h_l$ mit konstanten irreduziblen $q_i \in R$ und irreduziblen Polynomen h_i mit $\deg h_i \geq 1$ ist, dann gilt auch $C(f) \approx q_1 \dots q_k$. Wegen der Eindeutigkeit der Zerlegung in R folgt $k = n$, und es gibt eine Permutation $\pi \in S_n$ mit $p_i \approx q_{\pi(i)}$. Durch Kürzen erhält man $g_1 \dots g_m = (u h_1) \dots h_l$.
$g_1, \dots, g_m, u h_1, \dots, h_l$ sind irreduzibel in $R[x]$, und sie sind primitiv, also sind sie auch irreduzibel in $Q[x]$. Aufgrund der Eindeutigkeit der Zerlegung in $Q[x]$ gilt damit $m = l$, und es gibt eine Permutation $\sigma \in S_m$ mit $g_i \approx h_{\sigma(i)}$ in $Q[x]$. Weil $g_i, h_{\pi(i)}$ jedoch primitiv sind, gilt dies auch in $R[x]$. ∎

Korollar 12.8 Sei R ein ZPE-Ring, dann ist $R[x_1, \dots, x_n]$ ein ZPE-Ring.

Beweis: Mit Induktion, da $R[x_1, \dots, x_n] = R[x_1, \dots, x_{n-1}][x_n]$. ∎

Beispiel: $\mathbb{Z}[x]$ und $K[x, y]$ (K Körper) sind ZPE-Ringe und wegen Übung 30 keine Hauptidealringe.

Bemerkung: Sei R ein ZPE-Ring, Q sein Quotientenkörper und $\frac{a}{b} \in Q$, dann gibt es a', $b' \in R$, sodass $\mathrm{ggT}(a', b') = 1$ und $\frac{a}{b} = \frac{a'}{b'}$ (gekürzte Darstellung), nämlich $d = \mathrm{ggT}(a, b)$, $a = a'd$, $b = b'd$.

Lemma 12.9 Sei R ein ZPE-Ring, Q sein Quotientenkörper, $f(x) = \sum_{k=0}^{n} a_k x^k \in R[x]$. Wenn $\frac{c}{d} \in Q$ mit $\mathrm{ggT}(c, d) = 1$ und $f(\frac{c}{d}) = 0$, dann gilt $c \mid a_0$ und $d \mid a_n$.

Beweis: Aus $\sum_{k=0}^{n} a_k \frac{c^k}{d^k} = 0$ ergibt sich durch Multiplikation mit d^n:
$\sum_{k=0}^{n} d^{n-k} a_k c^k = 0$. Damit ist

$$a_0 d^n = -a_1 c d^{n-1} - a_2 c^2 d^{n-2} - \ldots - a_n c^n$$

Weil c die rechte Seite teilt, muss es auch $a_0 d^n$ teilen, weil aber $\mathrm{ggT}(c,d) = 1$ ist, folgt $c \mid a_0$.
Andererseits ist

$$a_n c^n = -a_0 d^n - a_1 c d^{n-1} - \ldots - a_{n-1} d c^{n-1}$$

Weil d die rechte Seite teilt, muss es auch $a_n c^n$ teilen, weil aber $\mathrm{ggT}(c,d) = 1$ ist, folgt $d \mid a_n$. ∎

Satz 12.10 (Eisensteinsches Irreduzibilitätskriterium) *Sei R ein ZPE-Ring, Q sein Quotientenkörper. Sei weiters $f = \sum_{k=0}^{n} a_k x^k \in R[x]$ mit $\deg f \geq 1$. Wenn es ein irreduzibles $p \in R$ gibt, sodass $p \nmid a_n$, $p \mid a_i$ für $i = 0, \ldots, n-1$, und $p^2 \nmid a_0$, dann ist f irreduzibel in $Q[x]$.*

Beweis: $f = C(f)\tilde{f}$, $\tilde{f} = \sum_{k=0}^{n} a'_k x^k$. Wegen $p \nmid a_n = C(f)a'_n$ gilt $p \nmid a'_n$, analog $p^2 \nmid a'_0$.
Wegen $p \nmid a_n$ teilt p auch $C(f)$ nicht, daher gilt wegen $p \mid a_i = C(f)a'_i$ auch $p \mid a'_i$ für $i = 0, \ldots, n-1$. Wir zeigen nun, dass $\tilde{f}$ in $D[x]$ irreduzibel ist:
Angenommen, es wäre $\tilde{f} = gh$, wobei $g, h \in D[x]$ keine Einheiten sind. Dann ist $\deg g \geq 1$ und $\deg h \geq 1$ (eine Konstante, die $\tilde{f}$ teilt, teilt auch $C(\tilde{f}) = 1$).
Sei $g = \sum_{k=0}^{m} b_k x^k$ mit $b_m \neq 0$ und $h = \sum_{k=0}^{l} c_k x^k$ mit $c_l \neq 0$. Es gilt $m, l \geq 1$, also auch $m, l < n$, weil $m + l = n$.
$p^2 \nmid a'_0 = b_0 c_0$, aber $p \mid a'_0$, daher teilt p genau eines der Elemente b_0, c_0, o.B.d.A. $p \mid b_0$, $p \nmid c_0$.
Sei k minimal, sodass $p \nmid b_k$ (existiert, weil p nicht alle a'_i teilt). Dann ist $0 < k \leq m < n$.
Es ist jedoch $a'_k = b_0 c_k + b_1 c_{k-1} + \ldots + b_k c_0$. Weil $p \mid a'_k$ und $p \mid b_i$ für $i < k$ gilt, folgt damit aber $p \mid b_k c_0$, also entweder $p \mid b_k$ oder $p \mid c_0$, ein Widerspruch.
Damit ist gezeigt, dass $\tilde{f}$ in $D[x]$ irreduzibel ist; da es primitiv ist, ist es auch irreduzibel in $K[x]$; weil zudem $\tilde{f} \approx f$ in $K[x]$, ist f auch irreduzibel in $K[x]$. ∎

Beispiel: $3x^3 + 12x^2 + 18 \in \mathbb{Z}[x]$ ist ($p = 2$) irreduzibel in $\mathbb{Q}[x]$ (aber nicht in $\mathbb{Z}[x]$!).

Bemerkung: Dieser Satz ermöglicht die Konstruktion von irreduziblen Polynomen beliebig hohen Grades über einem ZPE-Ring wie z.B. $\mathbb{Z}$.

Übungsbeispiele

Übung 48: In einem kommutativen Ring R gilt: d ist kgV von a und b genau dann, wenn

$$(a) \cap (b) = (d).$$

Übung 49: Sei R ein Hauptidealbereich. Dann gilt für Ideale A, B, C von R

$$A + (B \cap C) = (A + B) \cap (A + C) \quad \text{und} \quad A \cap (B + C) = (A \cap B) + (A \cap C)$$

Übung 50: Zeigen Sie durch Gegenbeispiele, daß weder $A+(B\cap C) = (A+B)\cap(A+C)$ noch $A \cap (B + C) = (A \cap B) + (A \cap C)$ für Ideale in einem ZPE-Ring gelten muß.

Übung 51: Sei R ein kommutativer Ring mit der Eigenschaft: zu je zwei verschiedenen Elementen a, b in R gibt es ein Polynom $f \in R[x]$ mit $f(a) = 1$, $f(b) = 0$. Dann ist R ein Körper.

Übung 52: Sei p eine Primzahl. Zeigen Sie mit Eisenstein, daß $f(x) = 1 + x + x^2 + \ldots + x^{p-1}$ irreduzibel in $\mathbb{Z}[x]$ und $\mathbb{Q}[x]$ ist. (Hinweis: $x^p - 1 = f(x)(x - 1)$; zeigen Sie $f(x + 1)$ irreduzibel. Einsetzen von $x + 1$ für x ist Automorphismus von $\mathbb{Z}[x]$.)

Übung 53: Formulieren Sie für einen Euklidischen Ring R einen Algorithmus zur Lösung von Kongruenzensystemen $x \equiv b_i \mod a_i$ mit $b_i \in R$ beliebig, $a_i \in R$ mit $\mathrm{ggT}(a_i, a_j) = 1$ für $i \neq j$, und demonstrieren Sie diesen durch Lösung des Systems

$$x \equiv 5 \mod 15 \quad x \equiv 2 \mod 11 \quad x \equiv 3 \mod 4$$

13 Chinesischer Restsatz

In diesem Kapitel sei R ein Ring mit 1, aber nicht notwendigerweise kommutativ.

Definition 13.1 Ideale I, $J \trianglelefteq R$ heißen *co-maximal* (oder *relativ prim*), wenn

$$I + J = R.$$

Bemerkung: Wir wissen: $I + J = R \Rightarrow I \cap J = IJ$. Mit Induktion folgt für Ideale A_i, $i \in \{i, \ldots, n\}$:

$$A_i + A_j = R \text{ für alle } i \neq j \Rightarrow \bigcap_{i=1}^{n} A_i = A_1 \cdot \ldots \cdot A_n$$

Lemma 13.2 Seien $A_1, \ldots, A_n$ Ideale von R mit $A_1 + A_j = R$ für $1 \neq j$, dann gilt

$$A_1 + A_2 A_3 \ldots A_n = R.$$

Beweis: Mit Induktion: Für $n = 2$ stimmt die Aussage

$n - 1 \to n$:

$$\begin{aligned} R = R^2 &= (A_1 + A_2 \ldots A_{n-1})(A_1 + A_n) \\ &= A_1^2 + A_2 \ldots A_{n-1} A_n + A_1 A_n + A_1 \ldots A_{n-1} \\ &\subseteq A_1 + A_2 \ldots A_n \end{aligned}$$

$\Rightarrow R = A_1 + A_2 \ldots A_n$. ∎

Satz 13.3 (Chinesischer Restsatz) *Sei R ein Ring mit 1 und $A_1, \ldots, A_n$ Ideale von R mit $A_i + A_j = R$ für $i \neq j$. Dann gilt: Gegeben $b_1, \ldots, b_m \in R$, dann gibt es $b \in R$, sodass $b \equiv b_i \mod A_i$ für $1 \leq i \leq n$. Dieses b ist eindeutig modulo $\bigcap_{i=1}^{n} A_i$.*

Beweis: Für alle i gilt $A_i + \bigcap_{j \neq i} A_j = R$, da $A_i + A_1 \ldots A_{i-1} A_{i+1} \ldots A_n = R$. Seien $c_i \in A_i$, $d_i \in \bigcap_{j \neq i} A_j$ mit $c_i + d_i = b_i$. Es gilt: $d_i \equiv b_i \mod A_i$ und $d_i \equiv 0 \mod A_j$ für $j \neq i$. Setze

$$b = d_1 + \ldots + d_n,$$

dann $b \equiv b_i \mod A_i$ für $1 \leq i \leq n$. Offensichtlich ist b eindeutig mod $\bigcap_{i=1}^{n} A_i$. ∎

Korollar 13.4 Seien $A_1, \ldots, A_n$ Ideale von R mit $A_i + A_j = R$ für $i \neq j$, dann gilt

$$R/(A_1 \ldots A_n) \simeq R/A_1 \times \ldots \times R/A_n .$$

Bemerkung: Allgemeiner gilt: Für beliebige Ideale $A_1, \ldots, A_n$ ist

$$\begin{aligned} &\varphi : R/(A_1 \cap \ldots \cap A_n) \to R/A_1 \times \ldots \times R/A_n \text{ definiert durch} \\ &\varphi(r + A_1 \cap \ldots \cap A_n) = (r + A_1, \ldots, r + A_n) \end{aligned}$$

ein Ringmonomorphismus. Für paarweise relativ prime Ideale liefert der Chinesische Restsatz die Surjektivität und $\bigcap_{i=1}^{n} A_i = A_1 \ldots A_n$.

Korollar 13.5 Seien $A_1, \ldots, A_n$ Ideale von R mit $A_i + A_j = R$ für $i \neq j$, dann gilt

$$[R : A_1 \ldots A_n] = [R : A_1] \ldots [R : A_n].$$

Nun untersuchen wir die Lösbarkeit von Kongruenzensystemen $x \equiv b_i \mod A_i$ für $1 \leq i \leq n$, wenn $A_i + A_j \neq R$. In diesem Fall ist nicht jedes System lösbar.

Beispiel:

$$\begin{aligned} x &\equiv 2 \mod 6 \qquad (\Rightarrow x \equiv 0 \mod 2) \\ x &\equiv 1 \mod 4 \qquad (\Rightarrow x \equiv 1 \mod 2) \end{aligned}$$

ist unlösbar.

Bemerkung: Eine notwendige Bedingung für die Lösbarkeit von

$$\begin{aligned} x &\equiv b_1 \mod n_1 \\ x &\equiv b_2 \mod n_2 \end{aligned}$$

ist

$$b_1 \equiv b_2 \mod \mathrm{ggT}(n_1, n_2).$$

In beliebigen Ringen mit 1 ist für die Lösbarkeit von $x \equiv b_i \mod A_i$ $(1 \leq i \leq n)$ notwendig:

$$b_i \equiv b_j \mod A_i + A_j \text{ für } i \neq j$$

(wenn $b \equiv b_i \mod A_i$, $b \equiv b_j \mod A_j$, dann folgt $b_i \equiv b \equiv b_j \mod A_i + A_j$).

Wir charakterisieren nun jene Ringe, in denen die notwendige Bedingung

$$b_i \equiv b_j \mod A_i + A_j$$

für die Lösbarkeit des Systems $x \equiv b_i \mod A_i$ auch hinreichend ist.

Lemma 13.6 Wenn für alle Ideale A, B, C von R gilt $(A + B) \cap (A + C) = A + (B \cap C)$, dann gilt auch für alle Ideale A, A_i von R:

$$\bigcap_{i=1}^{n} (A + A_i) = A + \bigcap_{i=1}^{n} A_i.$$

Beweis: durch Induktion ∎

Satz 13.7 *Sei R ein Ring mit 1. Dann sind folgende Aussagen äquivalent:*

1. *$\forall A, B, C \trianglelefteq R$:* $(A + B) \cap (A + C) = A + (B \cap C)$

2. $\forall A_1, \ldots, A_n \trianglelefteq R$: $\forall b_1, \ldots, b_n \in R$ *mit* $b_i \equiv b_j \mod A_i + A_j$:
   $\exists b \in R$ *mit* $b \equiv b_i \mod A_i$.

3. $(A \cap B) + (A \cap C) = A \cap (B + C)$

Beweis:
$(1 \Rightarrow 2)$: Induktion nach n:

$n = 2$: Es gelte $b_1 - b_2 \in A_1 + A_2$, also $b_1 - b_2 = a_1 + a_2$, mit $a_1 \in A_1$ und $a_2 \in A_2$. Setze $b := b_1 - a_1 = b_2 + a_2$. Dann ist $b \equiv b_1 \mod a_1$ und $b \equiv b_2 \mod a_2$.

$n-1 \to n$: Nach Induktionsvoraussetzung gibt es c, sodass $c \equiv b_i \mod A_i$ für $1 \leq i \leq n-1$. Es gilt $b_n \equiv b_i \equiv c \mod A_n + A_i$ für $1 \leq i \leq n-1$, also

$$c \equiv b_n \mod \bigcap_{i=1}^{n-1} (A_n + A_i) = A_n + \bigcup_{i=1}^{n-1} A_i.$$

Nach Induktionsvoraussetzung $(n = 2)$ ist

$$\begin{aligned} x &\equiv c \mod \bigcap_{i=1}^{n-1} A_i \\ x &\equiv b_n \mod A_n \end{aligned}$$

lösbar. Sei $b \in R$ eine Lösung des obigen Systems, dann gilt $b \equiv b_i$ für $1 \leq i \leq n$.

$(2 \Rightarrow 3)$: $(A \cap B) + (A \cap C) \subseteq A \cap (B + C)$ gilt in jedem Ring, zu zeigen bleibt also noch $A \cap (B + C) \subseteq (A \cap B) + (A \cap C)$.

Seien $a \in A$, $b \in B$, $c \in C$ gegeben mit $a = b + c$. Wir suchen $b' \in A \cap B$ und $c' \in A \cap C$, sodass $a = b' + c'$. Nach 2. ist folgendes Kongruenzensystem lösbar:

$$x \equiv 0 \mod A \qquad x \equiv b \mod B \qquad x \equiv b \mod C$$

($b \equiv 0 \mod A + B$, $b \equiv 0 \mod A + C$, da $b = a - c \in A + C$). Sei b' eine Lösung des Systems, d.h. $b' \equiv 0 \mod A$ und $b' \equiv b \mod B \cap C$. Dann gilt $a = b' + (a - b')$, wobei $b' \in A \cap B$ und $a - b' \in A \cap C$, da a, $b' \in A$ und $a - b' \equiv a - b = c \equiv 0 \mod C$.

$(3 \Rightarrow 1)$:

$$\begin{aligned} &(A + B) \cap (A + C) = ((A + B) \cap A) + ((A + B) \cap C) = \\ &= A + ((A + B) \cap C) = A + ((A \cap C) + (B \cap C)) = A + (B \cap C) \end{aligned}$$

Bemerkung: In Hauptidealringen gilt $(A + B) \cap (A + C) = A + (B \cap C)$ (Übung). Insbesondere gilt also der Chinesische Restsatz für nicht relativ prime Ideale für $\mathbb{Z}$ und für $K[x]$ (K Körper).

Allgemein heißen Ringe mit obiger Eigenschaft *arithmetische Ringe*, das heißt ein Ring R ist arithmetisch genau dann, wenn der Idealverband von R distributiv ist.

Definition 13.8 Ein *Verband* ($l$attice) ist eine Menge mit Ordnungsrelation $(X, \leq)$, in der es zu je zwei Elementen $a, b \in X$ ein Supremum und ein Infimum gibt. (c heißt *Supremum* von a und b, wenn $c \geq a$, $c \geq b$ und $\forall d \in X: \ (d \geq a \wedge d \geq b \Rightarrow d \geq c)$. u heißt *Infimum* von a und b, wenn $u \leq a$, $u \leq b$ und $\forall d \in X: \ (d \leq a \wedge d \leq b \Rightarrow d \leq u)$.)

Bemerkung: Wegen der Antisymmetrie von $\leq$ sind sup und inf, wenn sie existieren, eindeutig. Man schreibt $a \wedge b$ für $\inf(a, b)$ („meet“) und $a \vee b$ für $\sup(a, b)$ („join“).

Beispiel: Ideale eines Ringes, Untergruppen einer Gruppe, Normalteiler einer Gruppe bilden jeweils einen Verband: Die Ordnungsrelation ist $\subseteq$ (Inklusion), $\wedge = \cap$ (Durchschnitt), $\vee$ ist Erzeugnis (die von $A \cup B$ erzeugte Struktur).

- bei Idealen: $I \wedge J = I \cap J$, $I \vee J = I + J$
- bei Untergruppen: $H \wedge K = H \cap K$, $H \vee K = \langle H \cup K \rangle$
- bei Normalteilern (multiplikativ): $N \wedge M = N \cap M$, $N \vee M = NM$ ($\langle N \cup M \rangle = NM \Leftrightarrow NM = MN$)

Diese Verbände sind sogar vollständig.

Definition 13.9 Ein Verband $(X, \leq)$ heißt *vollständig*, wenn

$$\forall Y \subseteq X: \ \exists \sup Y \text{ und } \exists \inf Y$$

(s heißt $\sup Y$, wenn $\forall y \in Y: \ s \geq y$ und $\forall d \in X: \ ((\forall y \in Y: \ d \geq y) \Rightarrow d \geq s)$, inf analog mit $\leq$, statt $\geq$.)

Eine äquivalente Art, Verbände zu definieren, ist die folgende:

Definition 13.10 $(X, \wedge, \vee)$ heißt *Verband*, wenn folgende Axiome erfüllt sind:

V1) $a \wedge b = b \wedge a, \quad a \vee b = b \vee a$ (Kommutativität)

V2) $a \wedge (b \wedge c) = (a \wedge b) \wedge c, \quad a \vee (b \vee c) = (a \vee b) \vee c$ (Assoziativität)

V3) $a \wedge a = a, \quad a \vee a = a$

V4) $(a \wedge b) \vee a = a, \quad (a \vee b) \wedge a = a$

Diese beiden Definitionen sind äquivalent: Wenn $(X, \leq)$ eine geordnete Menge mit $\sup(a, b) =: a \vee b$ und $\inf(a, b) =: a \wedge b$ ist, dann erfüllen $\wedge$, $\vee$ die Axiome V1-V4.

Wenn $(X, \wedge, \vee)$ die Axiome V1-V4 erfüllt, dann gilt $a \wedge b = a \Leftrightarrow a \vee b = b$. Wenn man definiert:

$$a \leq b :\Leftrightarrow a \wedge b = a \text{ (oder äquivalent } a \vee b = b),$$

dann erhält man eine Ordnungsrelation und es gilt: $a \vee b = \sup(a, b)$, $a \wedge b = \inf(a, b)$.

Wenn man von einer geordneten Menge mit sup und inf ausgeht und durch $\wedge$ und $\vee$ wie oben $\leq$ definiert, bekommt man wieder die ursprüngliche Ordnungsrelation zurück.

Definition 13.11 Ein Verband $(X, \wedge, \vee)$ heißt *distributiv*, wenn

$$\forall a, b, c \in X : \ a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c),$$

oder, äquivalent

$$\forall a, b, c \in X : \ a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c).$$

Beweis (der Äquivalenz):
$\forall a, b, c \in X : \ a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c) \Rightarrow \forall a, b, c \in X : \ a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$
zeigt man wie $(3 \Rightarrow 1)$ in Satz 13.7:

$$(a \vee b) \wedge (a \vee c) = ((a \vee b) \wedge a) \vee ((a \vee b) \wedge c) = a \vee ((a \vee b) \wedge c) =$$
$$a \vee ((a \wedge c) \vee (b \wedge c)) = (a \vee (a \wedge c)) \vee (b \wedge c) = ((a \wedge c) \vee a) \vee (b \wedge c) = a \vee (b \wedge c)$$

$\forall a, b, c \in X : \ a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c) \Rightarrow \forall a, b, c \in X : \ a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$
bekommt man durch Dualisierung: Da die Verbandsaxiome symmetrisch in $\wedge$, $\vee$ sind, kann man, wenn man eine Aussage über $\wedge$, $\vee$ rein aus den Verbandsaxiomen hergeleitet hat, auch $\wedge$, $\vee$ vertauschen und erhält wieder eine gültige Aussage. ∎

Bemerkung: In verbandstheoretischen Worten lautet die Aussage aus Satz 13.7 über den Chinesischen Restsatz wie folgt: Genau für jene Ringe, deren Idealverband distributiv ist, ist die notwendige Bedingung $b_i \equiv b_j \mod A_i + A_j$ immer auch hinreichend für die Lösbarkeit des Kongruenzensystems $x \equiv b_i \mod A_i$ $(1 \leq i \leq n)$.

Übungsbeispiele

Übung 54: Sei K ein Körper und $a, b, c, d \in K$ mit $ad - bc \neq 0$. Dann ist das Einsetzen von $\frac{ax+b}{cx+d}$ für x ein Automorphismus von $K(x)$. Man bekommt alle Automorphismen dieser Form, wenn man sich auf $a, b, c, d \in K$ mit $ad - bc = 1$ beschränkt.

Übung 55: Zeigen Sie, dass in einem Verband (definiert als $(X, \wedge, \vee)$, sodaß die Axiome V1–V4 erfüllt sind) gilt

$$a \wedge b = a \iff a \vee b = b.$$

Übung 56: Ein Verband heißt modular, wenn gilt

$$a \geq b \Longrightarrow a \wedge (b \vee c) = b \vee (a \wedge c).$$

Zeigen Sie, daß der Normalteilerverband einer Gruppe G modular ist. Hinweis: der von Normalteilern A, B erzeugte Normalteiler ist $AB = \{ab \mid a \in A,\ b \in B\}$.

Übung 57: Sei K ein Körper und $\varphi\colon K \longrightarrow K$ ein Automorphismus. Dann ist die Menge der Fixpunkte von φ, $F = \{a \in K \mid \varphi(a) = a\}$, ein Körper.

Übung 58: Sei R ein ZPE-Ring mit Quotientenkörper K, und $f, g, h \in K[x]$ drei normierte Polynome (d.h. Leitkoeffizient jeweils 1), sodaß $f = g \cdot h$. Zeigen Sie: wenn $f \in R[x]$, dann auch $g, h \in R[x]$.

Übung 59:

(*i*) Sei $(X, \wedge, \vee)$ eine Menge mit zwei 2-wertigen Operationen, die V1–V4 erfüllen. Dann ist

$$a \leq b : \Longleftrightarrow \ a \wedge b = a$$

eine Ordnungsrelation auf X, bezüglich derer je zwei Elemente sup und inf haben, nämlich $sup(a, b) = a \vee b$ und $\inf(a, b) = a \wedge b$.

(*ii*) Sei $(X, \leq)$ eine geordnete Menge, in der je zwei Elemente sup und inf haben, dann erfüllen $a \wedge b := \inf(a, b)$ und $a \vee b := sup(a, b)$ die Bedingungen V1–V4.

Übung 60: Die vorhergehenden Beispiele zeigen, wie man aus $(X, \wedge, \vee)$ mit V1–V4 eine Ordnungsrelation auf X mit sup und inf konstruiert und umgekehrt. Zeigen Sie: wenn man diese Konstruktion zuerst in die eine Richtung und dann in die andere Richtung ausführt, dann bekommt man die ursprüngliche Struktur zurück, sowohl wenn man von $(X, \wedge, \vee)$ ausgeht, als auch, wenn man von $(X, \leq)$ ausgeht.

14 Direkte Summen und Produkte von Gruppen

Definition 14.1 (Direktes Produkt) Sei I eine nichtleere Menge und für jedes $i \in I$ eine Gruppe G_i gegeben. Das *direkte Produkt* der G_i ist

$$\prod_{i\in I} G_i := \{f : I \to \bigcup_{i\in I} G_i \mid f(i) \in G_i\}.$$

Die Elemente von $\prod_{i\in I} G_i$ schreibt man als $(g_i)_{i\in I}$ mit $g_i \in G_i$. Mit der Operation *komponentenweise Addition (bzw. Multiplikation)* ist $\prod_{i\in I} G_i$ eine Gruppe:

$$(g_i)_{i\in I} + (h_i)_{i\in I} = (g_i + h_i)_{i\in I} \qquad \text{(Gruppenoperation von } G_i \text{ in } i\text{-ter Komponente)}$$

Das neutrale Element von $\prod_{i\in I} G_i$ ist $(0_{G_i})_{i\in I}$. Das inverse Element zu $(g_i)_{i\in I}$ ist $(-g_i)_{i\in I}$.

Analoges gilt für multiplikative Notation.

Definition 14.2 Sei G_i eine Gruppe für $i \in I$, $\prod_{i\in I} G_i$ das direkte Produkt. Für $j \in I$ heißt

$$p_j : \prod_{i\in I} G_i \to G_j \text{ mit } p_j((g_i)_{i\in I}) = g_j$$

die *Projektion* auf den j-ten Faktor G_j und

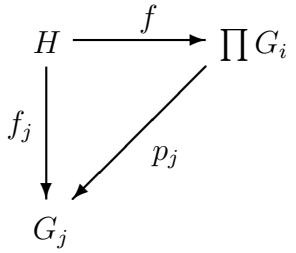
$$\varepsilon_j : G_j \to \prod_{i\in I} G_i \text{ mit } \varepsilon_j(g) = (g_i)_{i\in I}, \text{ wobei } g_i = \begin{cases} g & i = j \\ e_{G_i} & i \neq j \end{cases}$$

die *Einbettung* des j-ten Faktors G_j in $\prod_{i\in I} G_i$.

Proposition 14.3 p_j ist ein Gruppenepimorphismus, ε_j ist ein Gruppenmonomorphismus. $\widetilde{G}_j = \{(g_i)_{i\in I} \mid g_i = e_{G_i} \text{ für } i \neq j\} = \operatorname{Im} \varepsilon_j \simeq G_j$ ist ein Normalteiler von $\prod_{i\in I} G_i$.

Beweis: als Übung. ∎

Satz 14.4 (Universelle Eigenschaft des direkten Produkts) *Für $i \in I$ sei G_i eine Gruppe, $P = \prod_{i\in I} G_i$, $p_j : P \to G_j$ die Projektion auf den j-ten Faktor. Dann gilt:*
Für alle Gruppen H und alle Mengen $\{f_i : H \to G_i \mid i \in I\}$ von Gruppenhomomorphismen gibt es genau einen Homomorphismus $f : H \to P$ mit $\forall j \in I\ p_j \circ f = f_j$, d.h. das folgende Diagramm kommutiert:



Beweis: $p_j(f(h)) = f_j(h)\ \forall j \ \Rightarrow\ f(h) = (f_i(h))_{i\in I}$, also kann es höchstens einen solchen Homomorphismus geben, nämlich $f : H \to P$ definiert durch $f(h) = (f_i(h))_{i\in I}$. Dann gilt tatsächlich für alle j: $p_j(f(h)) = p_j((f_i(h))_{i\in I}) = f_j(h)$. Es bleibt noch zu zeigen, dass f ein Homomorphismus ist:

$$f(hk) = (f_i(hk))_{i\in I} = (f_i(h)f_i(k))_{i\in I} = (f_i(h))_{i\in I}(f_i(k))_{i\in I} = f(h)f(k)$$

Definition 14.5 (Direkte Summe) Sei $I \neq \emptyset$ eine Menge und für jedes $i \in I$ eine Gruppe G_i gegeben. Die *direkte Summe* der G_i, $\sum_{i\in I} G_i$ (oder $\bigoplus_{i\in I} G_i$), ist

$$\{(a_i)_{i\in I} \,|\, a_i \in G_i \text{ für } i \in I \wedge \text{ nur für endlich viele } i \in I \text{ ist } a_i \neq e_{G_i}\}$$

mit der komponentenweisen Multiplikation $(a_i)_{i\in I} \cdot (b_i)_{i\in I} = (a_ib_i)_{i\in I}$.
Sie kann als Untergruppe von $\prod_{i\in I} G_i$ aufgefasst werden:

$$\sum_{i\in I} G_i = \{(a_i)_{i\in I} \in \prod_{i\in I} G_i \,|\, \text{für höchstens endlich viele } i \in I \text{ ist } a_i \neq e_{G_i}\}$$

Definition 14.6 Sei G_i eine Gruppe für $i \in I$, $\sum_{i\in I} G_i$ die direkte Summe. Für $j \in I$ heißt

$$p_j : \sum_{i\in I} G_i \to G_j \text{ mit } p_j((g_i)_{i\in I}) = g_j$$

die *Projektion* auf den j-ten Summanden G_j und

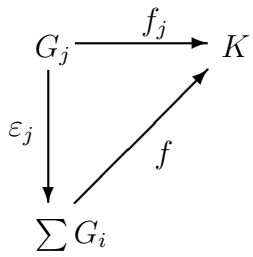
$$\varepsilon_j : G_j \to \sum_{i\in I} G_i \text{ mit } \varepsilon_j(g) = (g_i)_{i\in I}, \text{ wobei } g_i = \begin{cases} g & i = j \\ e_{G_i} & i \neq j \end{cases}$$

die *Einbettung* des j-ten Summanden G_j in $\sum_{i\in I} G_i$.

Proposition 14.7 p_j ist ein Gruppenepimorphismus, ε_j ist ein Gruppenmonomorphismus. $\widetilde{G}_j = \{(g_i)_{i\in I} \,|\, g_i = e_{G_i} \text{ für } i \neq j\} = \operatorname{Im}\varepsilon_j \simeq G_j$ ist ein Normalteiler von $\sum_{i\in I} G_i$. $\sum_{i\in I} G_i = \langle \bigcup_{j\in I} \widetilde{G}_j \rangle$ und $\forall j\ \widetilde{G_j} \cap \langle \bigcup_{j\in I, i\neq j} \widetilde{G}_j \rangle = \{e\}$.

Beweis: als Übung. ∎

Satz 14.8 (Universelle Eigenschaft der direkten Summe) *Sei $I \neq \emptyset$ eine Menge und für $i \in I$ sei $(G_i, +)$ eine Gruppe. Dann gilt für alle kommutativen Gruppen $(K, +)$ und alle Mengen $\{f_i : G_i \to K \,|\, i \in I\}$ von Gruppenhomomorphismen, dass es genau einen Homomorphismus $f : \sum_{i\in I} G_i \to K$ mit $\forall j \in I\ f \circ \varepsilon_j = f_j$ gibt, d.h. das folgende Diagramm kommutiert:*



BEMERKUNG: Für $(g_i)_{i\in I} \in \sum_{i\in I} G_i$ sei $\mathrm{Supp}((g_i)_{i\in I}) := \{i \in I \mid g_i \neq 0\}$ der *Träger* von $(g_i)_{i\in I}$.

Konvention: Die Summe einer leeren Menge von Elementen einer kommutativen Gruppe sei das Null-Element.

Beweis: Sei $g = (g_i)_{i\in I}$ und $\{i_1, \ldots, i_n\}$ derart, dass $g_i = 0$ für alle $i \notin \{i_1, \ldots, i_n\}$ ist. Dann ist $g = \varepsilon_{i_1}(g_{i_1}) + \ldots + \varepsilon_{i_n}(g_{i_n})$, und es muss daher gelten:

$$f(g) = f(\varepsilon_{i_1}(g_{i_1})) + \ldots + f(\varepsilon_{i_n}(g_{i_n})) = f_{i_1}(g_{i_1}) + \ldots + f_{i_n}(g_{i_n})$$

Also gibt es höchstens einen solchen Homomorphismus, nämlich $f : \sum_{i\in I} G_i \to K$ mit $f((g_i)_{i\in I}) = f_{i_1}(g_{i_1}) + \ldots + f_{i_n}(g_{i_n})$ für $\{i_1, \ldots, i_n\} = \mathrm{Supp}\, g$ (und $f(0) = 0$). Weil K kommutativ ist, kommt es dabei nicht auf die Reihenfolge der Summanden an, f ist daher jedenfalls wohldefiniert. Es bleibt jedoch zu zeigen, dass f ein Homomorphismus ist:
Seien dazu $g = (g_i)_{i\in I}$ und $h = (h_i)_{i\in I}$ gegeben und $\{i_1, \ldots, i_n\} = (\mathrm{Supp}\, g) \cup (\mathrm{Supp}\, h)$.

$$\begin{aligned}
f((g_i)_{i\in I} + (h_i)_{i\in I}) &= f((g_i + h_i)_{i\in I}) \\
&= f_{i_1}(g_{i_1} + h_{i_1}) + \ldots + f_{i_n}(g_{i_n} + h_{i_n}) \\
&= f_{i_1}(g_{i_1}) + f_{i_1}(h_{i_1}) + \ldots + f_{i_n}(g_{i_n}) + f_{i_n}(h_{i_n}) \\
&\overset{K \text{ kommutativ}}{=} f_{i_1}(g_{i_1}) + \ldots + f_{i_n}(g_{i_n}) + f_{i_1}(h_{i_1}) + \ldots + f_{i_n}(h_{i_n}) \\
&= f((g_i)_{i\in I}) + f((h_i)_{i\in I})
\end{aligned}$$

■

BEMERKUNG: In $\sum_{i\in I} G_i$ gilt für alle $i \in I$, dass $\tilde{G}_i = \varepsilon_i(G_i) = \{(g_i)_{i\in I} \mid \forall k \neq i : \ g_k = 0\}$ ein Normalteiler. Ausserdem gilt für alle $k \in I$: $\tilde{G}_k \cap \langle \bigcup_{i\neq k} \tilde{G}_i \rangle = \{0\}$ und $\sum_{i\in I} G_i$ wird erzeugt von $\bigcup_{i\in I} \tilde{G}_i$.

Satz 14.9 (Innere direkte Summe) *Sei $(G, +)$ eine Gruppe, $I \neq \emptyset$ eine Menge und für $i \in I$ sei $N_i \leq G$. Wenn die Bedingungen*

1. $\forall i \in I \ N_i \trianglelefteq G$
2. $\forall j \in I \ N_j \cap \langle \bigcup_{i\in I, i\neq j} N_i \rangle = \{0\}$
3. $G = \langle \bigcup_{i\in I} N_i \rangle$

gleichzeitig gelten, dann gilt

(a) *Für $g_i \in N_i$, $g_j \in N_j$ mit $i \neq j$ ist $g_i + g_j = g_j + g_i$.*

(b) *Jedes $g \in G$ hat eine Darstellung $g = g_{i_1} + \ldots + g_{i_n}$ mit $g_{i_k} \in N_{i_k}$ und $i_k \neq i_j$ für $k \neq j$.*

(c) *Diese Darstellung ist bis auf die Reihenfolge und eventuell eingefügte Summanden $g_{i_j} = 0$ eindeutig.*

Außerdem ist dann $\sum_{i\in I} N_i \simeq G$, wobei $\varphi : \sum_{i\in I} N_i \to G$ mit $\varphi((g_i)_{i\in I}) = g_{i_1} + \ldots + g_{i_n}$ (dabei ist $\{i_1, \ldots, i_n\} = \{i \in I \mid g_i \neq 0\} =: \operatorname{Supp} g$) der Isomorphismus ist.

Beweis:

(a) Nach 1. und 2. sind N_i und N_j Normalteiler mit trivialem Durchschnitt und kommutieren daher elementweise.

(b) Wegen 3. hat jedes $g \in G$ eine Darstellung der Form $g = g_{i_1} + \ldots + g_{i_n}$, wobei die i_k aber nicht notwendigerweise verschieden sein müssen. Wegen (a) kann man die g_{i_k} aber so vertauschen, dass alle g_{i_k} aus demselben N_i nebeneinanderstehen. Dann kann man sie zu einem Element zusammenfassen.

(c) Angenommen, es sei $g_{i_1} + \ldots + g_{i_k} = g'_{i_1} + \ldots + g'_{i_k}$ mit $g_{i_j}, g'_{i_j} \in N_{i_j}$, wobei die i_j paarweise verschieden seien (gegebenenfalls stellt man geeignet um und fügt Nullen ein, um links und rechts Elemente derselben Gruppen stehen zu haben). Dann folgt:

$$-g'_{i_1} + g_{i_1} = g'_{i_2} + \ldots + g'_{i_k} - g_{i_2} - \ldots - g_{i_k} \in N_{i_1} \cap \langle \bigcup_{i\in I, i\neq i_1} N_i \rangle$$

Wegen 2. muss daher $-g'_{i_1} + g_{i_1} = 0$, also $g'_{i_1} = g_{i_1}$, sein. Nun kann man auf beiden Seiten kürzen und erhält induktiv, dass $g'_{i_j} = g_{i_j}$ für alle j ist.

Sei nun φ wie oben definiert, wobei $\varphi(0) = 0$ gesetzt wird. Dann ist φ wegen (b) und (c) bijektiv. Es bleibt zu zeigen, dass φ ein Homomorphismus ist:
Zunächst sei bemerkt, dass für ein Element $(g_i)_{i\in I} \in \sum_{i\in I} N_i$ und eine beliebige endliche Menge $\{j_1, \ldots, j_m\}$, die $\operatorname{Supp} g$ enthält, auch $\varphi((g_i)_{i\in I}) = g_{j_1} + \ldots + g_{j_m}$ ist, da ja $g_{j_k} = 0$ für ein $j_k \notin \operatorname{Supp} g$ ist.
Seien nun $(g_i)_{i\in I}$, $(h_i)_{i\in I}$ zwei Elemente von $\sum_{i\in I} N_i$ und $K = \{k_1, \ldots, k_m\} =: (\operatorname{Supp} g) \cup (\operatorname{Supp} h)$. Dann ist jedenfalls für alle $i \in I \setminus K$ $g_i + h_i = 0$, d.h. $i \notin \operatorname{Supp}(g + h)$, also $\operatorname{Supp}(g + h) \subseteq K$. Es folgt:

$$\begin{aligned}
\varphi((g_i)_{i\in I} + (h_i)_{i\in I}) &= \varphi((g_i + h_i)_{i\in I}) \\
&= (g_{k_1} + h_{k_1}) + \ldots + (g_{k_m} + h_{k_m}) \\
&\overset{(*)}{=} g_{k_1} + \ldots + g_{k_m} + h_{k_1} + \ldots + h_{k_m} \\
&= \varphi((g_i)_{i\in I}) + \varphi((h_i)_{i\in I})
\end{aligned}$$

Man beachte, dass g_{k_l} und h_{k_l} nicht kommutieren müssen, der Schritt $(*)$ ist also keineswegs trivial. Man kann dennoch leicht von der einen auf die Darstellung kommen: hinter jedem h_{k_l} stehen nur Elemente aus den Gruppen N_i mit $i > k_l$, daher kann man der Reihe nach alle h_{k_l} durch geeignete Vertauschungen nach hinten verschieben, bis alle g_{k_r} vor allen h_{k_l} stehen. ∎

15 Freie Abelsche Gruppen

BEMERKUNG: Im folgenden werden alle Gruppen Abelsch (kommutativ) sein und additiv geschrieben werden.

Definition 15.1 Eine Teilmenge X einer kommutativen Gruppe A heißt *Basis* von A, wenn gilt:

- $\langle X \rangle = A$ (X ist Erzeugendensystem von A)
- Für alle paarweise verschiedenen $x_1, \ldots, x_n \in X$ und alle $k_1, \ldots, k_n \in \mathbb{Z}$ gilt: aus $k_1 x_1 + \ldots + k_n x_n = 0$ folgt $\forall i : k_i = 0$ (X ist $\mathbb{Z}$-linear unabhängige Menge)

Eine Abelsche Gruppe, die eine Basis besitzt, heißt *freie Abelsche Gruppe*.

BEMERKUNG: Nicht jede Abelsche Gruppe ist frei. Eine endliche Gruppe G kann z.B. nicht einmal eine 1-elementige $\mathbb{Z}$-linear unaghängige Teilmenge haben, weil für jedes $x \in G$ gilt: $\exists k \in \mathbb{Z} : \ k \neq 0$ und $kx = 0$.

Also sind endliche Gruppen $\neq \{0\}$ nicht frei Abelsch. $\{0\}$ gilt als frei Abelsch mit $\emptyset$ als Basis.

Auch $(\mathbb{Q}, +)$ und $(\mathbb{R}, +)$ sind keine freien Abelschen Gruppen.

Satz 15.2 *Sei A eine kommutative Gruppe. Dann sind folgende Aussagen äquivalent:*

- *A hat eine Basis $X = \{x_i \mid i \in I\} \neq \emptyset$.*
- *A ist innere direkte Summe der unendlichen zyklischen Untergruppen $\langle x_i \rangle$.*
- *$\sum_{i \in I} \mathbb{Z} \simeq A$ mit einem Isomorphismus $\varphi : \sum_{i \in I} \mathbb{Z} \to A$, der $\varphi(e_i) = x_i$ erfüllt. Dabei ist $e_i = (k_j)_{j \in I}$ mit $k_j = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases}$.*

Beweis:

- (1. $\Rightarrow$ 2.): Da X $\mathbb{Z}$-linear unabhängig ist, gilt $\forall x \in X, \ k \in \mathbb{Z} \ kx = 0 \Rightarrow k = 0$, daher ist $\langle x \rangle$ unendlich. Wegen der Kommutativität von A ist $\langle x \rangle$ für alle $x \in X$ ein Normalteiler, und es gilt $A = \langle \bigcup_{x \in X} \langle x \rangle \rangle$, da $A = \langle X \rangle$.
  Es bleibt noch zu zeigen, dass für alle $i \in I$ $\langle x_i \rangle \cap \langle \bigcup_{j \neq i} \langle x_j \rangle \rangle = \{0\}$ gilt. Sei dazu $a \in \langle x_i \rangle \cap \langle \bigcup_{j \neq i} \langle x_j \rangle \rangle$. Dann gibt es $j_1, \ldots, j_m \in I \setminus \{i\}$ und $k_1, \ldots, k_m, l \in \mathbb{Z}$ mit $a = l x_i = k_1 x_{j_1} + \ldots + k_m x_{j_m}$. Es folgt

$$k_1 x_{j_1} + \ldots + k_m x_{j_m} - l x_i = 0 \Rightarrow k_r = 0, l = 0 \Rightarrow a = 0$$

- (2. $\Rightarrow$ 3.): Wir definieren $\varphi : \sum_{i\in I}\mathbb{Z} \to A$ durch $\varphi((k_i)_{i\in I}) = k_{i_1}x_{i_1} + \ldots + k_{i_n}x_{i_n}$, wobei $\{i_1, \ldots, i_n\} = \{i \in I \mid k_i \neq 0\}$. Dann ist φ surjektiv, weil $X \subseteq \operatorname{Im}\varphi \leq A$ gilt. φ ist injektiv, weil X $\mathbb{Z}$-linear unabhängig ist und somit

$$\begin{aligned} & k_{i_1}x_{i_1} + \ldots + k_{i_n}x_{i_n} = l_{i_1}x_{i_1} + \ldots + l_{i_n}x_{i_n} \\ \Rightarrow\ & (k_{i_1} - l_{i_1})x_{i_1} + \ldots + (k_{i_n} - l_{i_n})x_{i_n} = 0 \\ \Rightarrow\ & k_{i_j} = l_{i_j} \end{aligned}$$

  gilt. φ ist ein Homomorphismus, weil A kommutativ ist und somit

$$\begin{aligned} \varphi((k_i + l_i)_{i\in I}) &= (k_{i_1} + l_{i_1})x_{i_1} + \ldots + (k_{i_n} + l_{i_n})x_{i_n} \\ &= k_{i_1}x_{i_1} + \ldots + k_{i_n}x_{i_n} + l_{i_1}x_{i_1} + \ldots + l_{i_n}x_{i_n} \\ &= \varphi((k_i)_{i\in I}) + \varphi((l_i)_{i\in I}) \end{aligned}$$

  folgt.

- (3. $\Rightarrow$ 1.): Wir zeigen dazu, dass $(e_i)_{i\in I}$ eine Basis von $\sum_{i\in I}\mathbb{Z}$ ist: wenn $(k_i)_{i\in I}$ ein Element von $\sum_{i\in I}\mathbb{Z}$ ist, dann lässt es sich als $(k_i)_{i\in I} = k_{i_1}e_{i_1} + \ldots + k_{i_n}e_{i_n}$ mit $\{i_1, \ldots, i_n\} = \{i \in I \mid k_i \neq 0\}$ schreiben. Also ist $(e_i)_{i\in I}$ ein Erzeugendensystem.
  Ist andererseits $k_{i_1}e_{i_1} + \ldots + k_{i_n}e_{i_n} = 0$, wobei die i_j paarweise verschieden sind, dann folgt $(l_i)_{i\in I} = 0$ mit

$$l_i = \begin{cases} k_{i_j} & i = i_j \in \{i_1, \ldots, i_n\} \\ 0 & \text{sonst} \end{cases}$$

  also $l_i = 0$ $\forall i$ und in weiterer Folge $k_{i_j} = 0$ $\forall j$. Also ist $(e_i)_{i\in I}$ auch $\mathbb{Z}$-linear unabhängig. ∎

Satz 15.3 *Sei A eine freie Abelsche Gruppe mit Basis X. Dann gibt es für alle Abelschen Gruppen B und alle Funktionen $f : X \to B$ genau einen Gruppenhomomorphismus $\overline{f} : A \to B$ mit $\overline{f}|_X = f$ (bzw. $\overline{f} \circ \operatorname{incl}_{X\hookrightarrow A} = f$).*

Beweis: Da X ein Erzeugendensystem von A ist, folgt für zwei Gruppenhomomorphismen $\overline{f}, \overline{g}$ mit $\overline{f}|_X = \overline{g}|_X$ auch, dass $\overline{f} = \overline{g}$ auf ganz A gilt. Also gibt es höchstens einen solchen Gruppenhomomorphismus.
Sei andererseits $\overline{f}$ durch

$$\overline{f}(k_1x_{i_1} + \ldots + k_nx_{i_n}) = k_1f(x_{i_1}) + \ldots + k_nf(x_{i_n})$$

gegeben. Dann ist $\overline{f}$ wohldefiniert, weil jedes $x \in A$ genau eine Darstellung der Form $k_1x_{i_1} + \ldots + k_nx_{i_n}$ hat. Die Tatsache $\overline{f}|_X = f$ ist unmittelbar ersichtlich, und dass es sich um einen Gruppenhomomorphismus handelt, lässt sich leicht nachprüfen. Also gibt es tatsächlich einen eindeutigen Homomorphismus, der die Bedingungen erfüllt. ∎

Satz 15.4 *Die Kardinalität einer Basis einer freien Abelschen Gruppe ist eindeutig: Für Basen X, Y gilt:* $|X| = |Y|$.

Beweis: Wir unterscheiden die folgenden beiden Fälle:

1. Es gibt eine endliche Basis $X \subseteq A$. In diesem Fall betrachten wir

   $$\mathrm{Hom}(A, \mathbb{Z}_2) = \{\overline{f} : A \to \mathbb{Z}_2 \,|\, \overline{f} \text{ ist Gruppenhomomorphismus}\}.$$

   Nach vorigem Satz gibt es eine Bijektion $\varphi : \mathbb{Z}_2^X \to \mathrm{Hom}(A, \mathbb{Z}_2)$, der jeder Funktion $f : X \to \mathbb{Z}_2$ einen Homomorphismus $\varphi(f) = \overline{f}$ zuordnet. Also ist

   $$|\mathrm{Hom}(A, \mathbb{Z}_2)| = |\mathbb{Z}_2^X| = 2^{|X|}.$$

   Für jede weitere Basis Y muss ebenso $|\mathrm{Hom}(A, \mathbb{Z}_2)| = 2^{|Y|}$ gelten. Es folgt dann $2^{|X|} = 2^{|Y|} \Rightarrow |X| = |Y|$.

2. Alle Basen sind unendlich. In diesem Fall zeigen wir, dass für jede unendliche Basis X $|X| = |A|$ gilt. Dabei ist $|X| \leq |A|$ klar, weil $X \subseteq A$ ist.
   Für $x \in X$ gilt $|\langle x \rangle| = |\mathbb{Z}| = \aleph_0$. Sei nun $S = \bigcup_{n \in \mathbb{N}} X^n$ und für $s = (x_1, \ldots, x_n) \in S$

   $$A_s = \langle x_1, \ldots, x_n \rangle = \langle x_1 \rangle \oplus \ldots \oplus \langle x_n \rangle \simeq \mathbb{Z} \oplus \ldots \oplus \mathbb{Z}$$

   Dann ist $|A_s| = |\mathbb{Z}^n| = \aleph_0$ und $A = \bigcup_{s \in S} A_s$, also $|A| \leq |S| \cdot \aleph_0$. Weil $|X^n| = |X|$ für unendliches X gilt, folgt weiters $|S| \leq |\mathbb{N}| \cdot |X| = |X|$ und damit

   $$|A| \leq |S| \cdot \aleph_0 \leq |X| \cdot \aleph_0 = |X|$$

   ($|X| \cdot \aleph_0 = |X|$, falls X unendlich ist). ∎

Bemerkung: Seien λ, κ unendliche Kardinalzahlen. Dann gilt $\lambda + \kappa = \max(\lambda, \kappa)$ und $\lambda \cdot \kappa = \max(\lambda, \kappa)$. Wenn also κ unendlich ist (d.h. $\kappa \geq \aleph_0$), dann $\kappa \cdot \aleph_0 = \kappa$ und $\kappa^n = \kappa \cdot \ldots \cdot \kappa = \kappa$.

Definition 15.5 Sei A eine freie Abelsche Gruppe und X eine Basis von A. Dann heißt $|X|$ der *Rang* von A.

Satz 15.6 *Sei G eine Abelsche Gruppe mit Erzeugendensystem $X \subseteq G$ und F eine freie Abelsche Gruppe vom Rang $|X|$. Dann gibt es einen Gruppenepimorphismus $\varphi : F \to G$.*

Insbesondere ist jede endlich erzeugte Abelsche Gruppe homomorphes Bild einer freien Abelschen Gruppe von endlichem Rang.

Beweis: Sei F frei Abelsch mit Basis X', $|X'| = |X|$. Sei $\psi : X' \to X$, $\psi(x') = x$ eine Bijektion, dann kann ψ zu einem Gruppenepimorphismus $\varphi : F \to G$ fortgesetzt werden. (surjektiv, weil $X \subseteq \mathrm{Im}\,\varphi \leq G$ und $\langle X \rangle = G$) ∎

Korollar 15.7 Jede endlich erzeugte Abelsche Gruppe G ist isomorph zu F/H, wobei F frei Abelsch von endlichem Rang und $H \leq F$.

Übungsbeispiele

Übung 61: $(\mathbb{Q}^+, \cdot)$ ist isomorph zu einer direkten Summe von abzählbar unendlich vielen Kopien von $(\mathbb{Z}, +)$ und daher frei Abelsch. ($\mathbb{Q}^+ = \{x \in \mathbb{Q} \mid x > 0\}$)

Übung 62: $(\mathbb{Q}, +)$ ist nicht frei Abelsch. Hinweis: je zwei Elemente $\mathbb{Z}$-linear abhängig, und $(\mathbb{Q}, +)$ nicht isomorph zu $(\mathbb{Z}, +)$.

Übung 63: $(\mathbb{R}, +)$ ist nicht frei Abelsch. Hinweis: Eine Basis als freie Abelsche Gruppe wäre auch Basis von $\mathbb{R}$ als $\mathbb{Q}$-Vektorraum, und wegen Eindeutigkeit der Koeffizienten dann aber kein Erzeugendensystem von $(\mathbb{R}, +)$ als Abelscher Gruppe.

Übung 64: Sei R ein Hauptidealring und $a, b \in R$ mit $\mathrm{ggT}(a, b) = d$. Zeigen Sie, dass man jede Matrix $\begin{pmatrix} a & b \\ * & * \end{pmatrix}$ durch Multiplikation von rechts mit einer Matrix $C \in \mathrm{SL}_2(R)$ auf die Form $\begin{pmatrix} d & 0 \\ * & * \end{pmatrix}$ bringen kann.

Übung 65: Eine Elementarmatrix (über R) ist eine Matrix der Form $E_{ij} = I + \lambda e_{ij}$, wobei I die Einheitsmatrix ist, $\lambda \in R$, $i \neq j$ und e_{ij} die Matrix, die an der Stelle (i, j) die Eintragung 1 hat und sonst nur 0.

Zeigen Sie

(i) $E_{ij}(\lambda)E_{ij}(\mu) = E_{ij}(\lambda + \mu)$

und daher $E_{ij}(\lambda)^{-1} = E_{ij}(-\lambda)$. (Die Relationen $(i) - (iii)$ in diesem und dem folgenden Beispiel heissen Steinberg-Relationen.)

Übung 66: Mit $[x, y]$ bezeichnen wir den Kommutator von x und y, d.h. $[x, y] = xyx^{-1}y^{-1}$. Zeigen Sie

(ii) $[E_{ij}(\lambda), E_{jk}(\mu)] = E_{ik}(\lambda\mu)$ für $i \neq k$,

(iii) $[E_{ij}(\lambda), E_{lk}(\mu)] = 1$, wenn $j \neq l$, $i \neq k$.

Hinweis: $e_{ij}e_{jk} = e_{ik}$ und $e_{ij}e_{kl} = 0$ für $j \neq k$.

16 Matrixumformungen mit Elementaroperationen

Definition 16.1 Sei R ein Ring und $A \in M_{n\times m}(R)$. Eine *elementare Zeilenoperation* ist das Addieren des λ-fachen der j-ten Zeile zur i-ten Zeile von A für $i \neq j$ und $\lambda \in R$.

Analog ist eine *elementare Spaltenoperation* das Addieren des λ-fachen der j-ten Spalte zur i-ten Spalte von A für $i \neq j$ und $\lambda \in R$.

Definition 16.2 Eine *Elementarmatrix* über R ist eine Matrix, die sich von der Einheitsmatrix nur durch eine Eintragung $\lambda \in R$ an einer Stelle (i, j) mit $i \neq j$ unterscheidet. $E_{ij}(\lambda)$ $(i \neq j)$ ist die Elementarmatrix mit Eintrag λ in Zeile i, Spalte j, Einträgen 1 in der Diagonale und sonst 0.

$$E_{ij}(\lambda)_{kl} = \begin{cases} 1, & \text{wenn } k = l \\ \lambda, & \text{wenn } k = i,\ l = j \\ 0, & \text{sonst} \end{cases}$$

Bemerkung: Addition des λ-fachen der j-ten Zeile zur i-ten Zeile entspricht einer Multiplikation von A mit der Matrix $E_{ij}(\lambda)$ von links $(A \mapsto E_{ij}(\lambda) \cdot A)$.

Addition des λ-fachen der j-ten Spalte zur i-ten Spalte entspricht einer Multiplikation von A mit der Matrix $E_{ji}(\lambda)$ von rechts $(A \mapsto A \cdot E_{ji}(\lambda))$.

Lemma 16.3 Sei $A \in M_{n\times m}(R)$. Eine Vertauschung der Zeilen i und j von A mit anschließender Multiplikation einer der beiden Zeilen mit (-1) ist durch elementare Zeilenumformungen erreichbar. Analoges gilt auch für Spalten.

Beweis: Folgende Zeilenoperationen führen zum gewünschten Ergebnis:

- Addiere i-te Zeile zur j-ten Zeile.
- Addiere das (-1)-fache der j-ten Zeile zur i-ten Zeile.
- Addiere i-te Zeile zur j-ten Zeile.

Analog für Spalten. ∎

Lemma 16.4 Sei A eine $n \times m$-Matrix mit Eintragungen in einem Euklidischen Ring R. Durch elementare Zeilen- und Spaltenumformungen kann A auf eine Form $A' = (a'_{ij})$ gebracht werden, wobei a'_{11} alle Eintragungen von A' teilt.

Beweis: O.B.d.A. darf angenommen werden, dass A nicht die Nullmatrix ist (andernfalls erfüllt A bereits die Bedingung). Dann lässt sich durch elementare Zeilen- und Spaltenumformungen $a_{11} \neq 0$ erreichen. Wir behaupten nun, dass wir A auf eine Form $B = (b_{ij})$

mit $\rho(b_{11}) < \rho(a_{11})$ bringen können, wenn a_{11} noch nicht alle Einträge teilt. Ist diese Behauptung gezeigt, dann folgt das Gewünschte, denn da die Folge $\rho(a_{11}) > \rho(b_{11}) > \ldots$ nur endlich sein kann, bricht diese Umformungskette nach endlich vielen Schritten ab, sodass dann a'_{11} tatsächlich alle Einträge teilt.
Der Beweis dieser Behauptung erfolgt in zwei Schritten:

1. Falls a_{11} nicht alle Eintragungen der ersten Zeile und der ersten Spalte teilt (o.B.d.A. sei ersteres der Fall), dann gibt es ein j, sodass $a_{11} \nmid a_{1j}$. Wir können eine Division mit Rest durchführen: $a_{1j} = qa_{11} + r$ mit $r \neq 0$ und $\rho(r) < \rho(a_{11})$. Wir ziehen nun das q-fache der ersten Spalte von der j-ten Spalte ab. Dann steht r in der Position $(1, j)$ und lässt sich durch Vertauschung in die erste Spalte bringen. Wir erhalten ein B mit $\rho(b_{11}) = \rho(r) < \rho(a_{11})$.

2. Falls a_{11} alle Eintragungen der ersten Zeile und der ersten Spalte teilt, kann man derart elementare Zeilen- und Spaltenumformungen machen, dass in der ersten Zeile und Spalte außer a_{11} nur noch Nullen stehen. Wir erhalten eine Matrix B, in der a_{11} genau dann b_{ij} teilt, wenn a_{11} a_{ij} teilt (bei allen Umformungen wurden stets nur Vielfache von a_{11} abgezogen). An zumindest einer Stelle muss daher ein b_{ij} stehen, das von a_{11} nicht geteilt wird. Durch Addition der i-ten Zeile zur ersten Zeile kann man diesen Eintrag in die erste Zeile bringen, wobei an der Stelle $(1, 1)$ weiterhin a_{11} steht. Damit haben wir das Problem auf den ersten Fall zurückgeführt. ∎

Satz 16.5 *Sei A eine $n \times m$-Matrix über einem Euklidischen Ring R. Dann kann A durch elementare Zeilen- und Spaltenumformungen auf Diagonalform $B = \mathrm{diag}(b_1, \ldots, b_k)$ $(k = \min(n, m))$ gebracht werden, sodass $b_1 \mid b_2 \mid \ldots \mid b_k$.*

Beweis: Wir führen eine Induktion nach $\max(m, n)$ durch: falls $\max(m, n) = 1$ ist, hat die Matrix bereits die gewünschte Form. Andernfalls sei A eine Matrix mit $max(m, n) > 1$. Durch elementare Zeilen- und Spaltenoperationen kann man A auf die Form $A' = (a'_{ij})$ mit $a'_{11} \mid a'_{ij}$ für alle i, j bringen (nach dem vorigen Lemma). Dann ist $a'_{1j} = q_j a'_{11}$ und $a'_{j1} = r_j a'_{11}$. Für alle $j > 1$ zieht man nun das q_j-fache der ersten Spalte von der j-ten Spalte und das r_j-fache der ersten Zeile von der j-ten Zeile ab. Dadurch werden in der ersten Zeile und in der ersten Spalte alle Einträge außer dem ersten zu 0.
Wir erhalten eine Matrix B mit $b_{11} = a'_{11}$ als einzigem Element $\neq 0$ in der ersten Zeile bzw. Spalte. Alle übrigen Einträge haben die Form $b_{ij} = a'_{ij} - q_j a'_{i1} = a'_{ij} - q_j r_i a'_{11}$ und sind daher durch $a'_{11} = b_{11}$ teilbar. Wenn man nun also die erste Zeile und Spalte von B weglässt, so kann man auf die verbliebene Matrix C die Induktionsvoraussetzung anwenden: C kann durch elementare Zeilen- und Spaltenoperationen auf Diagonalgestalt $\mathrm{diag}(c_1, \ldots, c_l)$ mit $c_1 \mid c_2 \mid \ldots \mid c_l$ gebracht werden, wobei diese Operationen auch gleich auf ganz B angewandt werden können. Sie ändern auch nichts an der Tatsache, dass b_{11} alle Einträge von C teilt. Man erhält daher wie gewünscht eine Matrix der Gestalt $\mathrm{diag}(b_{11}, c_1, \ldots, c_l)$ mit $b_{11} \mid c_1 \mid \ldots \mid c_l$. ∎

17 Struktur endlich erzeugter Abelscher Gruppen

Lemma 17.1 Sei $(M, +)$ eine Abelsche Gruppe, M' eine Untergruppe. Wenn sowohl M' als auch M/M' die Eigenschaft haben, dass jede Untergruppe endlich erzeugt ist, dann hat auch M diese Eigenschaft.

Beweis: Sei $N \leq M$. Dann ist $N \cap M'$ endlich erzeugt durch gewisse $n_1, \ldots, n_s \in N \cap M'$, und auch $\overline{N} = (N + M')/M'$ ist endlich erzeugt durch gewisse $l_1 + M', \ldots, l_t + M'$ mit $l_1, \ldots, l_t \in N$.
$l_1, \ldots, l_t, n_1, \ldots, n_s$ erzeugen dann N: sei dazu $g \in N$. Dann ist $g + M' = r_1(l_1 + M') + \ldots + r_t(l_t + M')$ für gewisse $r_1, \ldots, r_t \in \mathbb{Z}$. Damit lässt sich g in der Form

$$g = r_1 l_1 + \ldots + r_t l_t + m'$$

mit einem $m' \in M'$ (das auch in N liegen muss, da $g, l_1, \ldots, l_t$ in N liegen) darstellen. Es gibt daher $k_1, \ldots, k_s \in \mathbb{Z}$, sodass $m' = k_1 n_1 + \ldots + k_s n_s$. Es folgt

$$g = r_1 l_1 + \ldots + r_t l_t + k_1 n_1 + \ldots + k_s n_s$$

Satz 17.2 *Jede Untergruppe einer endlich erzeugten Abelschen Gruppe ist endlich erzeugt.*

Beweis: Sei M erzeugt durch $m_1, \ldots, m_t$. Wir führen eine Induktion nach t durch:

- Für $t = 1$ ist M zyklisch. Wir wissen bereits, dass dann jede Untergruppe auch zyklisch ist.
- Die Behauptung gelte für alle Gruppen mit $t - 1$ Erzeugern. Sei nun $M' = \langle m_t \rangle$. Dann wird M/M' von den $t - 1$ Elementen $m_i + M'$ $(i = 1, \ldots, t - 1)$ erzeugt. Nach Induktionsvoraussetzung ist jede Untergruppe von M' und jede Untergruppe von M/M' endlich erzeugt. Nach dem vorigen Lemma ist somit jede Untergruppe von M endlich erzeugt. ∎

Lemma 17.3 Seien $(F, +)$ eine Abelsche Gruppe und $v_1, \ldots, v_n \in F$. Dann gelten die folgenden Aussagen:

(i) Seien $1 \leq i, j \leq n$, $i \neq j$ und $\lambda \in \mathbb{Z}$. Wenn $w_j = v_j + \lambda v_i$ und $w_k = v_k$ für $k \neq j$ definiert werden, dann erzeugen $v_1, \ldots, v_n$ und $w_1, \ldots, w_n$ dieselbe Untergruppe von F.

(ii) Wenn $w_1, \ldots, w_n$ und $v_1, \ldots, v_n$ wie oben gewählt werden, dann sind $w_1, \ldots, w_n$ genau dann $\mathbb{Z}$-linear unabhängig, wenn $v_1, \ldots, v_n$ $\mathbb{Z}$-linear unabhängig sind.

(iii) Insbesondere gilt: $w_1, \ldots, w_n$ sind genau dann eine Basis von F, wenn $v_1, \ldots, v_n$ eine Basis von F sind.

Beweis: als Übung. ∎

Lemma 17.4 Sei $(F, +)$ eine freie Abelsche Gruppe mit Basis $e_1, \ldots, e_n$, und $w_1, \ldots, w_m \in F$. Wenn $A \in M_{m \times n}(\mathbb{Z})$ jene Matrix ist, deren k-te Zeile die Koeffizienten von w_k zur Basis $e_1, \ldots, e_n$ enthält, d.h. $w_k = a_{k1}e_1 + \ldots + a_{kn}e_n$, dann gilt:

(i) $A \cdot E_{ji}(\lambda)$ ist jene Matrix, deren k-te Zeile die Koeffizienten von w_k zur Basis $e'_1, \ldots, e'_n$ mit $e'_j = e_j - \lambda e_i$ und $e'_l = e_l$ $(l \neq j)$ enthält.

(ii) $E_{ij}(\lambda) \cdot A$ ist jene Matrix, deren k-te Zeile die Koeffizienten von w'_k zur Basis $e_1, \ldots, e_n$ mit $w'_i = w_i + \lambda w_j$ und $w'_l = w_l$ $(l \neq i)$ enthält.

Beweis: als Übung. ∎

Satz 17.5 *Sei $(F, +)$ eine freie Abelsche Gruppe vom Rang n, G eine Untergruppe. Dann existieren eine Basis $e_1, \ldots, e_n$ von F und $d_1, \ldots, d_n \in \mathbb{N}_0$ mit $d_1 \mid \ldots \mid d_n$, sodass $G = \langle d_1 e_1, \ldots, d_n e_n \rangle$. Insbesondere ist G eine freie Abelsche Gruppe mit Basis $d_1 e_1, \ldots, d_k e_k$, wobei d_k der letzte Wert $\neq 0$ ist.*

Beweis: G ist als Untergruppe einer endlich erzeugten Gruppe endlich erzeugt, und zwar durch Elemente $g_1, \ldots, g_m$. Dabei darf angenommen werden, dass $m \geq n$ ist, da man sonst beliebige Elemente von G hinzufügen kann. Sei $A = (a_{ij})$ die Matrix der Koeffizienten der g_i zur Basis $e_1, \ldots, e_n$, d.h. $g_i = a_{i1}e_1 + \ldots + a_{in}e_n$.
A kann durch elementare Spaltenoperationen (was einem Übergang zu einer anderen Basis von F entspricht) und elementare Zeilenoperationen (was einem Übergang zu einem anderen Erzeugendensystem von G entspricht) sowie durch Zeilen- und Spaltenvertauschungen (welche einem Umordnen der Basis von F bzw. des Erzeugendensystems von G entsprechen) auf die Form $A' = \operatorname{diag}(d_1, \ldots, d_n)$ mit $d_1 \mid \ldots \mid d_n$ gebracht werden, wobei A' wieder eine Matrix von Koeffizienten von einem Erzeugendensystem von G zu einer Basis von F ist; d.h., es existiert eine Basis $e'_1, \ldots, e'_n$, sodass $g'_i = a'_{i1}e'_1 + \ldots + a'_{in}e'_n$ $(1 \leq i \leq n)$ ein Erzeugendensystem von G ist. Wegen der speziellen Gestalt von A' ist $g'_i = d_i e'_i$ mit $d_1 \mid \ldots \mid d_n$. ∎

Lemma 17.6 Sei $I \neq \emptyset$ eine Menge und für jedes $i \in I$ seien Gruppen G_i, H_i und ein Homomorphismus $f_i : G_i \to H_i$ gegeben. Dann ist $f =: \sum_{i \in I} f_i : \sum_{i \in I} G_i \to \sum_{i \in I} H_i$, definiert durch $f((g_i)_{i \in I}) = (f_i(g_i))_{i \in I}$, ein Gruppenhomomorphismus mit

$$\operatorname{Ker} f = \{(g_i)_{i \in I} \mid g_i \in \operatorname{Ker} f_i \ \forall i\} = \sum_{i \in I} \operatorname{Ker} f_i$$

und

$$\operatorname{Im} f = \{(h_i)_{i \in I} \mid h_i \in \operatorname{Im} f_i \ \forall i\} = \sum_{i \in I} \operatorname{Im} f_i$$

Insbesondere ist f genau dann ein Epi- bzw. Monomorphismus, wenn alle f_i Epi- bzw. Monomorphismen sind.

Insbesondere gilt: Wenn $N_i \trianglelefteq G_i$ für $i \in I$, dann ist $\sum_{i\in I} N_i \trianglelefteq \sum_{i\in I} G_i$, und es gilt

$$\left(\sum_{i\in I} G_i\right) \Big/ \left(\sum_{i\in I} N_i\right) \simeq \sum_{i\in I} {}^{G_i}\!/_{N_i} .$$

Beweis: als Übung. ∎

Korollar 17.7 Sei F eine freie Abelsche Gruppe vom Rang n und $G \leq F$ eine Untergruppe von F, dann gibt es $r, s \in \mathbb{N}_0$ mit $r + s \leq n$ und $m_1, \ldots, m_r \in \mathbb{Z}$ mit $m_1 \mid m_2 \mid \ldots \mid m_r$ und $m_i \notin \{0, 1\}$, sodass

$$ {}^{F}\!/_{G} \simeq {}^{\mathbb{Z}}\!/_{m_1\mathbb{Z}} \times \ldots \times {}^{\mathbb{Z}}\!/_{m_r\mathbb{Z}} \times \mathbb{Z} \times \ldots \times \mathbb{Z} \quad (s \text{ Faktoren } \mathbb{Z}).$$

Beweis: Wir wenden das Lemma an auf $G = \langle d_1 v_1, \ldots, d_n v_n\rangle \leq F = \langle v_1\rangle \oplus \ldots \oplus \langle v_n\rangle$. Es gilt $\langle d_i v_i\rangle \leq \langle v_i\rangle$ und daher

$$ {}^{F}\!/_{G} \simeq {}^{\langle v_1\rangle}\!/_{\langle d_1 v_1\rangle} \oplus \ldots \oplus {}^{\langle v_n\rangle}\!/_{\langle d_n v_n\rangle} \simeq {}^{\mathbb{Z}}\!/_{d_1\mathbb{Z}} \times \ldots \times {}^{\mathbb{Z}}\!/_{d_n\mathbb{Z}}$$

mit $d_1 = \ldots = d_k = 1$, d_{k+1}, …, $d_{k+r} \in \mathbb{N} \setminus \{0, 1\}$ und $d_{k+r+1} = \ldots = d_n = 0$. Setze $m_1 := d_{k+1}, \ldots, m_r = d_{k+r}$ und $s := n - k - r$. Es gilt

$$ {}^{\mathbb{Z}}\!/_{1\,\mathbb{Z}} \simeq \{0\}, \quad {}^{\mathbb{Z}}\!/_{0\mathbb{Z}} \simeq \mathbb{Z},$$

und somit

$$ {}^{F}\!/_{G} \simeq {}^{\mathbb{Z}}\!/_{m_1\mathbb{Z}} \times \ldots \times {}^{\mathbb{Z}}\!/_{m_r\mathbb{Z}} \times \mathbb{Z} \times \ldots \times \mathbb{Z} \quad (s \text{ Faktoren } \mathbb{Z}).$$

Satz 17.8 *Sei G eine endlich erzeugte Abelsche Gruppe. Dann gibt es $m_1, \ldots, m_r \in \mathbb{N}$ $(r \geq 0)$ mit $m_1 \mid \ldots \mid m_r$ und $m_1 > 1$, sodass*

$$G \simeq Z_{m_1} \oplus \ldots \oplus \mathbb{Z}_{m_r} \oplus H$$

mit $H = \sum_{i=1}^{s} \mathbb{Z}$ $(s \geq 0)$ ist.

Bemerkung: In dieser Darstellung sind $m_1, \ldots, m_r$ und s eindeutig bestimmt (wird später bewiesen). $m_1, \ldots, m_r$ heißen *invariante Faktoren* von G.

Beweis: Sei G erzeugt von n Elementen und F die freie Abelsche Gruppe vom Rang n. Dann gibt es einen Epimorphismus $f : F \to G$. Sei K dessen Kern. Nach dem ersten Isomorphiesatz gilt dann $G \simeq {}^{F}\!/_{K}$. Nach dem vorigen Satz gibt es daher r, $s \in \mathbb{N}_0$ und $m_1, \ldots m_r \in \mathbb{N} \setminus \{1\}$, sodass $m_1 \mid \ldots \mid m_r$ und

$$G \simeq {}^{F}\!/_{K} \simeq {}^{\mathbb{Z}}\!/_{m_1\mathbb{Z}} \times \ldots \times {}^{\mathbb{Z}}\!/_{m_r\mathbb{Z}} \times \mathbb{Z} \times \ldots \times \mathbb{Z} \quad (s \text{ Faktoren } \mathbb{Z}).$$

Lemma 17.9 Für $m, n \in \mathbb{N}$ mit $\mathrm{ggT}(m,n) = 1$ gilt $\mathbb{Z}_{mn} \simeq \mathbb{Z}_m \oplus \mathbb{Z}_n$.

Beweis: Dieses Lemma ist eine unmittelbare Folgerung aus dem Chinesischen Restsatz, angewandt auf $\mathbb{Z}$. ∎

Korollar 17.10 Ist $m = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$, wobei $p_1, \ldots, p_k$ verschiedene Primzahlen und $\alpha_i \in \mathbb{N}$ sind, dann gilt

$$\mathbb{Z}_m \simeq \mathbb{Z}_{p_1^{\alpha_1}} \oplus \ldots \oplus \mathbb{Z}_{p_k^{\alpha_k}}$$

Beweis: durch Induktion nach k. ∎

Satz 17.11 *Sei G eine endlich erzeugte Abelsche Gruppe. Dann existieren Primzahlen $p_1, \ldots, p_k$ $(k \geq 0)$, $n_1, \ldots, n_k \in \mathbb{N}$, $\alpha_{ij} \in \mathbb{N}$ und $s \in \mathbb{N}_0$, sodass*

$$G \simeq \mathbb{Z}_{p_1^{\alpha_{11}}} \oplus \ldots \oplus \mathbb{Z}_{p_1^{\alpha_{1n_1}}} \oplus \ldots \oplus \mathbb{Z}_{p_k^{\alpha_{k1}}} \oplus \ldots \oplus \mathbb{Z}_{p_k^{\alpha_{kn_k}}} \oplus H$$

mit $H = \sum_{i=1}^{s} \mathbb{Z}$.

Beweis: Dieser Satz folgt aus $G \simeq \mathbb{Z}_{m_1} \oplus \ldots \oplus \mathbb{Z}_{m_r} \oplus H$ und $\mathbb{Z}_{m_i} \simeq \mathbb{Z}_{p_1^{\alpha_{1i}}} \oplus \ldots \oplus \mathbb{Z}_{p_k^{\alpha_{ki}}}$. ∎

Bemerkung: Die Potenzen $p_i^{\alpha_{ij}}$, die hierbei vorkommen, sind ebenso wie s eindeutig und heißen *Elementarteiler* von G.

Eindeutigkeit der invarianten Faktoren und Elementarteiler:

Lemma 17.12 Sei $(A, +)$ eine Abelsche Gruppe, $m \in \mathbb{N}$ und p eine Primzahl. Folgende Mengen sind Untergruppen von A:

1. Die *Torsionsuntergruppe* von A:

$$A_t = \{a \in A \,|\, \exists n \in \mathbb{N} : na = 0\} = \{a \in A \,|\, |a| \text{ ist endlich}\}$$

2. Für p prim:

$$A(p) = \{a \in A \,|\, \exists n \in \mathbb{N}_0 : \ |a| = p^n\} = \{a \in A \,|\, \exists n \in \mathbb{N}_0 : \ p^n a = 0\} = \bigcup_{n=0}^{\infty} A[p^n]$$

3. Für $m \in \mathbb{N}$:

$$A[m] = \{a \in A \,|\, ma = 0\} = \{a \in A \,|\, |a| \Big| m\}$$

4. Für $m \in \mathbb{N}$:

$$mA = \{ma \,|\, a \in A\}$$

BEMERKUNG: Für nichtkommutative Gruppen ist im Allgemeinen keine dieser Mengen eine Untergruppe!

Beweis: Alle diese Mengen sind nichtleer, da 0 enthalten ist. Wir zeigen jeweils $a, b \in G$ (wobei G die jeweilige Menge ist) $\Rightarrow a - b \in G$:

1. $ma = 0$, $nb = 0 \Rightarrow (mn)a = (mn)b = 0 \Rightarrow (mn)(a-b) = (mn)a - (mn)b = 0 - 0 = 0$
2. $p^n a = 0$, $p^m b = 0 \Rightarrow p^\mu a = p^\mu b = 0$ für $\mu = \max(m, n)$, also $p^\mu(a - b) = p^\mu a - p^\mu b = 0 - 0 = 0$
3. $ma = 0$, $mb = 0 \Rightarrow m(a - b) = ma - mb = 0 - 0 = 0$
4. $ma - mb = m(a - b)$ ∎

Lemma 17.13 Für die eben definierten Gruppen gelten folgende Zusammenhänge:

1. $\mathbb{Z}_{p^n}[p] \simeq \mathbb{Z}_p$
2. $p^m \mathbb{Z}_{p^n} \simeq \mathbb{Z}_{p^{n-m}}$ (für $m < n$)
3. $(\sum_{i\in I} G_i)[m] = \sum_{i\in I}(G_i[m])$ und $m \sum_{i\in I} G_i = \sum_{i\in I} mG_i$
4. Wenn $f : G \to H$ ein Gruppenisomorphismus ist, dann ist $f|_{G_t} : G_t \to H_t$ auch ein Gruppenisomorphismus, und für eine Primzahl p ist $f|_{G(p)} : G(p) \to H(p)$ ebenso ein Gruppenisomorphismus.

Beweis:

1. Es gilt $|\overline{p^{n-1}}| = p$ in $\mathbb{Z}_{p^n}$. Daher genügt es zu zeigen, dass $\mathbb{Z}_{p^n}[p] = \langle\overline{p^{n-1}}\rangle$ ist. Jedenfalls gilt $\langle\overline{p^{n-1}}\rangle \subseteq \mathbb{Z}_{p^n}[p]$. Ist andererseits $k \in \mathbb{Z}$ derart, dass $p\overline{k} = \overline{0}$ in $\mathbb{Z}_{p^n}$ gilt, dann muss $p^n | pk$ und in weiterer Folge $p^{n-1} | k$ gelten. Also ist $\overline{k} = m\overline{p^{n-1}}$ in $\mathbb{Z}_{p^n}$, und es folgt, dass $\mathbb{Z}_{p^n}[p]$ von $\overline{p^{n-1}}$ erzeugt wird.
2. $p^m \mathbb{Z}_{p^n} = \{p^m \overline{k} \,|\, k \in \mathbb{Z}\} = \{k\overline{p^m} \,|\, k \in \mathbb{Z}\} = \langle\overline{p^m}\rangle$; nun ist $|\overline{p^m}| = p^{n-m}$ in $\mathbb{Z}_{p^n}$, also ist $p^m \mathbb{Z}_{p^n}$ die zyklische Gruppe der Ordnung p^{n-m}.
3. folgt unmittelbar aus $m(a_i)_{i\in I} = (ma_i)_{i\in I}$
4. folgt aus der Tatsache, dass für einen Isomorphismus f $|f(g)| = |g|$ $\forall g \in G$ gilt. ∎

Lemma 17.14 Sei p eine Primzahl und

$$G \simeq \sum_{i=1}^{r} \mathbb{Z}_{p^{\alpha_i}} \simeq \sum_{j=1}^{r'} \mathbb{Z}_{p^{\beta_j}}$$

($r, r' \in \mathbb{N}$, $\alpha_i, \beta_j \in \mathbb{N}$). Dann gilt $r = r'$ und $\forall n \in \mathbb{N}$ $|\{i \,|\, \alpha_i = n\}| = |\{j \,|\, \beta_j = n\}|$.

Beweis: Wir zeigen, dass für alle n

$$a(n) := |\{i \,|\, \alpha_i \geq n\}| = |\{j \,|\, \beta_j \geq n\}| =: b(n)$$

gilt. Dann folgt die Behauptung wegen $|\{i \,|\, \alpha_i = n\}| = a(n) - a(n-1)$ und $|\{j \,|\, \beta_j = n\}| = b(n) - b(n-1)$.
Dazu zeigen wir, dass $|(p^{n-1}G)[p]| = p^{a(n)}$ gilt: $p^{n-1}\mathbb{Z}_{p^\alpha} \neq \{0\} \Leftrightarrow \alpha \geq n$; $G = \sum_{i=1}^{r} \mathbb{Z}_{p^{\alpha_i}}$. Also folgt

$$p^{n-1}G = \sum_{i=1}^{r} p^{n-1}\mathbb{Z}_{p^{\alpha_i}} \simeq \sum_{k=1}^{a(n)} p^{n-1}\mathbb{Z}_{p^{\alpha_{i_k}}} = \sum_{k=1}^{a(n)} \mathbb{Z}_{p^{\alpha_{i_k}-n+1}}$$

wobei die i_k genau jene sind, für die $\alpha_{i_k} \geq n$ ist. Daraus ergibt sich weiter

$$(p^{n-1}G)[p] = \sum_{k=1}^{a(n)} \mathbb{Z}_{p^{\alpha_{i_k}-n+1}}[p] \simeq \sum_{k=1}^{a(n)} \mathbb{Z}_p$$

und daher die Behauptung. Analog gilt auch $|(p^{n-1}G)[p]| = p^{b(n)}$ und damit

$$p^{a(n)} = p^{b(n)} \;\Rightarrow\; a(n) = b(n)$$

. ∎

Lemma 17.15 Sei G eine Abelsche Gruppe und $G \simeq H_1 \oplus G_1 \simeq H_2 \oplus G_2$, wobei G_1, G_2 endlich und H_1, H_2 frei Abelsch mit den Rängen s_1, s_2 sind. Dann gilt $G_1 \simeq G_2 \simeq G_t$, $H_1 \simeq H_2 \simeq G/G_t$ und $s_1 = s_2$.

Beweis: $(a, b) \in H_1 \oplus G_1$ hat genau dann endliche Ordnung, wenn $a = 0$ ist, also folgt $G_t \simeq (H_1 \oplus G_1)_t = \{0\} \oplus G_1 \simeq G_1$ und analog auch $G_2 \simeq G_t$. Es folgt weiters

$$G/G_t \simeq (H_1 \oplus G_1)/(\{0\} \oplus G_1) \simeq H_1/\{0\} \oplus G_1/G_1 \simeq H_1 \oplus \{0\} \simeq H_1$$

und analog $G/G_t \simeq H_2$, daher $H_1 \simeq H_2$ und $s_1 = s_2$. ∎

Satz 17.16 *Sei G eine endlich erzeugte Abelsche Gruppe. Dann gilt*

1. *In jeder Darstellung von G als direkte Summe zyklischer Gruppen ist die Anzahl der vorkommenden unendlichen Faktoren dieselbe.*
2. *Wenn*

$$\begin{aligned} G &\simeq \mathbb{Z}_{p_1^{\alpha_{11}}} \oplus \ldots \oplus \mathbb{Z}_{p_1^{\alpha_{1n_1}}} \oplus \ldots \oplus \mathbb{Z}_{p_k^{\alpha_{k1}}} \oplus \ldots \oplus \mathbb{Z}_{p_k^{\alpha_{kn_k}}} \oplus \sum_{i=1}^{s} \mathbb{Z} \\ &\simeq \mathbb{Z}_{p_1^{\beta_{11}}} \oplus \ldots \oplus \mathbb{Z}_{p_1^{\beta_{1m_1}}} \oplus \ldots \oplus \mathbb{Z}_{p_k^{\beta_{k1}}} \oplus \ldots \oplus \mathbb{Z}_{p_k^{\beta_{km_k}}} \oplus \sum_{i=1}^{s'} \mathbb{Z} \end{aligned}$$

gilt, wobei $p_1, \ldots, p_k$ verschiedene Primzahlen sind und $\alpha_{ij}, \beta_{ij} \in \mathbb{N}_0$, dann gilt $s = s'$, und für jedes p_i gilt

$$\forall n \in \mathbb{N}\ |\{j \mid \alpha_{ij} = n\}| = |\{j \mid \beta_{ij} = n\}|$$

(*Eindeutigkeit der Elementarteiler*).

3. *Wenn*

$$G \simeq \mathbb{Z}_{m_1} \oplus \ldots \oplus \mathbb{Z}_{m_r} \oplus \sum_{i=1}^{s} \mathbb{Z} \simeq \mathbb{Z}_{n_1} \oplus \ldots \oplus \mathbb{Z}_{n_t} \oplus \sum_{i=1}^{s'} \mathbb{Z}$$

mit $1 < m_1 \mid \ldots \mid m_r$ und $1 < n_1 \mid \ldots \mid n_t$ gilt, dann ist $r = t$, $s = s'$ und $m_i = n_i$ $(1 \leq i \leq r)$ (*Eindeutigkeit der invarianten Faktoren*).

Beweis:

1. Nach dem vorigen Lemma ist die Anzahl der unendlichen Faktoren gleich dem Rang von G/G_t, also in allen Darstellungen dieselbe.

2. Wegen 1. gilt $s = s'$ jedenfalls. Für alle i gilt weiters

$$G(p_i) \simeq \mathbb{Z}_{p_i^{\alpha_{i1}}} \oplus \ldots \oplus \mathbb{Z}_{p_i^{\alpha_{in_i}}} \simeq \mathbb{Z}_{p_i^{\beta_{i1}}} \oplus \ldots \oplus \mathbb{Z}_{p_i^{\beta_{im_i}}}$$

weil $|(a_1, \ldots, a_m)| = \mathrm{kgV}(|a_1|, \ldots, |a_m|)$ ist und dies somit nur genau dann eine Potenz von p_i sein kann, wenn $a_l = 0$ in allen Faktoren außer den $\mathbb{Z}_{p_i^k}$ ist. Nach dem Lemma 17.14 sind damit die vorhandenen Potenzen von p_i dieselben.

3. Wieder folgt $s = s'$ aus 1. Seien nun $p_1, \ldots, p_k$ die Potenzen, die eines der m_i oder n_i teilen. Nun kann man die m_i, n_i in der Form $m_i = \prod_{j=1}^{k} p_j^{\alpha_{ij}}$ bzw. $n_i = \prod_{j=1}^{k} p_j^{\beta_{ij}}$ schreiben. Es folgt

$$G \simeq \sum_{j=1}^{k} \sum_{i=1}^{r} \mathbb{Z}_{p_j^{\alpha_{ij}}} \oplus \mathbb{Z}^s \simeq \sum_{j=1}^{k} \sum_{i=1}^{t} \mathbb{Z}_{p_j^{\beta_{ij}}} \oplus \mathbb{Z}^s$$

Wegen 2. muss dann $\forall i\ \forall n\ |\{j \mid \alpha_{ij} = n\}| = |\{j \mid \beta_{ij} = n\}|$ gelten. Da m_i m_{i+1} teilen soll, wird m_r von allen übrigen m_i geteilt, also ergibt sich für alle j:

$$\alpha_{rj} = \max\{\alpha_{ij} \mid i = 1, \ldots, r\} = \max\{\beta_{ij} \mid i = 1, \ldots, t\} = \beta_{tj}$$

Daher ist $m_r = n_t$, analog dann $m_{r-1} = n_{t-1}$ etc. und $r = t$. ∎

Übungsbeispiele

Übung 67: Sei $I \neq \emptyset$ eine Menge und für jedes $i \in I$ seien Gruppen G_i, H_i und ein Homomorphismus $f_i : G_i \to H_i$ gegeben. Dann ist $f =: \sum_{i\in I} f_i : \sum_{i\in I} G_i \to \sum_{i\in I} H_i$, definiert durch $f((g_i)_{i\in I}) = (f_i(g_i))_{i\in I}$, ein Gruppenhomomorphismus mit

$$\operatorname{Ker} f = \{(g_i)_{i\in I} \mid g_i \in \operatorname{Ker} f_i \ \forall i\} = \sum_{i\in I} \operatorname{Ker} f_i$$

und

$$\operatorname{Im} f = \{(h_i)_{i\in I} \mid h_i \in \operatorname{Im} f_i \ \forall i\} = \sum_{i\in I} \operatorname{Im} f_i$$

Insbesondere ist f genau dann ein Epi- bzw. Monomorphismus, wenn alle f_i Epi- bzw. Monomorphismen sind.

Insbesondere gilt: Wenn $N_i \trianglelefteq G_i$ für $i \in I$, dann ist $\sum_{i\in I} N_i \trianglelefteq \sum_{i\in I} G_i$, und es gilt

$$\Big(\sum_{i\in I} G_i\Big) / \Big(\sum_{i\in I} N_i\Big) \simeq \sum_{i\in I} (G_i/N_i)$$

Übung 68: Seien $(F, +)$ eine Abelsche Gruppe und $v_1, \ldots, v_n \in F$. Dann gelten die folgenden Aussagen:

(*i*) Seien $1 \leq i, j \leq n$, $i \neq j$ und $\lambda \in \mathbb{Z}$. Wenn $w_j = v_j + \lambda v_i$ und $w_k = v_k$ für $k \neq j$ definiert werden, dann erzeugen $v_1, \ldots, v_n$ und $w_1, \ldots, w_n$ dieselbe Untergruppe von F.

(*ii*) Wenn $w_1, \ldots, w_n$ und $v_1, \ldots, v_n$ wie oben gewählt werden, dann sind $w_1, \ldots, w_n$ genau dann $\mathbb{Z}$-linear unabhängig, wenn $v_1, \ldots, v_n$ $\mathbb{Z}$-linear unabhängig sind.

(*iii*) Insbesondere gilt: $w_1, \ldots, w_n$ sind genau dann eine Basis von F, wenn $v_1, \ldots, v_n$ eine Basis von F sind.

Übung 69: Sei F eine freie Abelsche Gruppe mit Basis $e_1, \ldots, e_n$, und $w_1, \ldots, w_m \in F$. Wenn $A \in M_{m\times n}(\mathbb{Z})$ jene Matrix ist, deren k-te Zeile die Koeffizienten von w_k zur Basis $e_1, \ldots, e_n$ enthält, d.h. $w_k = a_{k1}e_1 + \ldots + a_{kn}e_n$, dann gilt:

(*i*) $A \cdot E_{ji}(\lambda)$ ist jene Matrix, deren k-te Zeile die Koeffizienten von w_k zur Basis $e'_1, \ldots, e'_n$ mit $e'_j = e_j - \lambda e_i$ und $e'_l = e_l$ $(l \neq j)$ enthält.

(*ii*) $E_{ij}(\lambda) \cdot A$ ist jene Matrix, deren k-te Zeile die Koeffizienten von w'_k zur Basis $e_1, \ldots, e_n$ mit $w'_i = w_i + \lambda w_j$ und $w'_l = w_l$ $(l \neq i)$ enthält.

Übung 70: Sei R ein kommutativer Ring und $u \in R$ eine Einheit. Zeigen Sie, daß man $\begin{pmatrix} u & 0 \\ 0 & u^{-1} \end{pmatrix}$ als Produkt von Elementarmatrizen darstellen kann. (Hinweis: durch elementare Zeilenoperationen in die Einheitsmatrix überführen; Inverse einer Elementarmatrix ist wieder Elementarmatrix.)

Übung 71: Sei R Euklidischer Ring. Zeigen Sie, daß jede Matrix in $\mathrm{SL}_n(R)$ Produkt von Elementarmatrizen ist. Hinweis: diagonalisieren und Bsp 70.

Übung 72: Sei F freie Abelsche Gruppe mit Basis w_1, w_2, w_3 und G die von den Elementen $g_1 = 2w_1 + w_2 - 3w_3$ und $g_2 = w_1 - w_2 + 2w_3$ erzeugte Untergruppe. Bestimmen Sie die Struktur von F/G.

Übung 73: Bestimmen Sie Elementarteiler und invariante Faktoren von

$$\mathbb{Z}_{120} \times \mathbb{Z}_{45} \times \mathbb{Z}_{28} \times \mathbb{Z}_{125}.$$

Übung 74: (*i*) Ist die Gruppe aus Bsp. 73 isomorph zu $\mathbb{Z}_{30} \times \mathbb{Z}_{225} \times \mathbb{Z}_8 \times \mathbb{Z}_7 \times \mathbb{Z}_{60}$?

(*ii*) Ist die Gruppe aus Bsp. 73 isomorph zu $\mathbb{Z}_{60} \times \mathbb{Z}_{56} \times \mathbb{Z}_{75} \times \mathbb{Z}_{90}$?

Übung 75: Skizzieren Sie einen Beweis, dass man jede $n \times k$ Matrix A über einem Hauptidealring R durch Multiplikation von links mit Matrizen aus $\mathrm{SL}_n(R)$ und von rechts mit Matrizen aus $\mathrm{SL}_k(R)$ auf Diagonalgestalt mit

$$a_{11} \mid a_{22} \ldots a_{ii} \mid a_{i+1i+1}$$

bringen kann. Hinweis: wie für Euklidischen Ring, mit Länge eines Elements $\ell(r)$ statt Rangfunktion $\rho(r)$, wobei $\ell(r)$ die Anzahl der Primelemente, deren Produkt r ist (mit Vielfachheiten), angibt. Zusätzlich zu Elementarmatrizen verwendet man Blockdiagonalmatrizen bestehend aus einer Matrix wie in Bsp. 64 und sonst Einsern auf der Diagonale.

18 Körpererweiterungen

Definition 18.1 Wenn F, K Körper mit $K \leq F$ sind, dann heißt das Paar K, F eine *Körpererweiterung* (geschrieben $F : K$). F heißt *Erweiterungskörper* von K.

Bemerkung: Wenn $F : K$ eine Körpererweiterung ist, dann ist F ein K-Vektorraum: $(F, +)$ ist eine Abelsche Gruppe, die Skalarmultiplikation $K \times F \to F$ ist die Einschränkung der Multiplikation in F auf Paare in $K \times F$.

Definition 18.2 Sei $F : K$ eine Körpererweiterung. Die Dimension von F als K-Vektorraum heißt *Grad* der Körpererweiterung $F : K$, man schreibt $[F : K] = \dim_K F$.

Lemma 18.3 Seien K, E, F Körper mit $K \leq E \leq F$; sei B eine Basis von F als E-Vektorraum, C eine Basis von E als K-Vektorraum. Dann ist $D = (d_{(c,b)})_{(c,b)\in C\times B}$ mit $d_{(c,b)} = cb$ eine Basis von F als K-Vektorraum.

Beweis: Sei $f \in F$. Dann gibt es Elemente $b_1, \ldots, b_n \in B$ und $e_1, \ldots, e_n \in E$, sodass $f = e_1b_1 + \ldots + e_nb_n$. Weiters existieren $c_1, \ldots, c_m \in C$ und $k_{ij} \in K$, sodass $e_i = \sum_{j=1}^m k_{ij}c_j$, also $f = \sum_{i=1}^n \sum_{j=1}^m k_{ij}c_jb_i$.
f ist daher K-Linearkombination von Elementen der Form c_jb_i, also ist D Erzeugendensystem.
D ist linear unabhängig über K: seien $c_1, \ldots, c_m \in C$, $b_1, \ldots, b_n \in B$, $k_{ij} \in K$, sodass $\sum_{1\leq i\leq n, 1\leq j\leq m} k_{ij}c_jb_i = 0$. Dann ist $\sum_{i=1}^n (\sum_{j=1}^m k_{ij}c_j)b_i = 0$, und der Ausdruck in der Klammer liegt für alle i in E. Da B eine E-linear unabhängige Menge ist, folgt $\sum_{j=1}^m k_{ij}c_j = 0$ für alle i und damit (da C linear unabhängig über K ist) auch $k_{ij} = 0$ für alle Paare i, j. Also muss D K-linear unabhängig sein. ∎

Korollar 18.4 Für Körper K, E, F mit $K \leq E \leq F$ gilt $[F : K] = [F : E][E : K]$.

Definition 18.5 Sei $F : K$ eine Körpererweiterung und $u \in F$. u heißt *algebraisch* über K, wenn $\exists f \in K[x]$, $f \neq 0$, mit $f(u) = 0$. Andernfalls, d.h., wenn aus $f \in K[x]$ und $f(u) = 0$ bereits $f = 0$ folgt, heißt u *transzendent* über K.

Beispiel: $i \in \mathbb{C}$ ist algebraisch über $\mathbb{Q}$: es ist Nullstelle von $x^2 + 1 \in \mathbb{Q}[x]$. $\sqrt{2} \in \mathbb{R}$ ist algebraisch über $\mathbb{Q}$: es ist Nullstelle von $x^2 - 2 \in \mathbb{Q}[x]$.

e, π sind hingegen transzendent über $\mathbb{Q}$.

Definition 18.6 Eine Körpererweiterung $F : K$ heißt *algebraisch*, wenn jedes $u \in F$ algebraisch über K ist. Andernfalls (d.h., wenn ein $u \in F$ existiert, das transzendent über K ist) heißt die Körpererweiterung *transzendent*.

Beispiel: $\mathbb{C} : \mathbb{R}$ ist eine algebraische Körpererweiterung, $\mathbb{R} : \mathbb{Q}$ ist eine transzendente Körpererweiterung.

Definition 18.7 Sei $F : K$ eine Körpererweiterung, $S \subseteq F$. Der von S über K *erzeugte Unterring* von F ist definiert als

$$K[S] = \bigcap_{\substack{R \text{ Ring} \\ K \cup S \subseteq R \subseteq F}} R$$

(dies ist einfach der von $K \cup S$ erzeugte Unterring von F).

Der von S über K *erzeugte Unterkörper* ist definiert als

$$K(S) = \bigcap_{\substack{E \text{ Körper} \\ K \cup S \subseteq E \subseteq F}} E$$

(der von $K \cup S$ erzeugte Unterkörper von F).

Bemerkung: $K(S)$ ist ebenso wie $K[S]$ wohldefiniert, da der Durchschnitt von Körpern wieder ein Körper ist (Beweis analog zu dem für Ringe).

Wenn $S = \{s_1, \ldots, s_n\}$, dann schreibt man $K[s_1, \ldots, s_n]$ für $K[\{s_1, \ldots, s_n\}]$ und $K(s_1, \ldots, s_n)$ für $K(\{s_1, \ldots, s_n\})$.

Satz 18.8 *Seien K, F Körper, $K \leq F$, $u, u_i \in F$ $(i = 1, \ldots, n)$ und $S \subseteq F$ (für die Aussagen 1.-3. genügt es, wenn F ein kommutativer Ring mit Eins ist). Dann gilt:*

1. $K[u] = \{a_0 + a_1 u + \ldots + a_n u^n \mid n \in \mathbb{N}_0, a_i \in K\} = \{f(u) \mid f \in K[x]\}$
2. $K[u_1, \ldots, u_n] = \{\sum_{(k_1,\ldots,k_n) \in \mathbb{N}_0^n} a_{(k_1,\ldots,k_n)} u_1^{k_1} \ldots u_n^{k_n} \mid a_{(k_1,\ldots,k_n)} \in K,$ *nur endlich viele* $a_{(k_1,\ldots,k_n)}$ *sind* $\neq 0\}$, *d.h.*

$$K[u_1, \ldots, u_n] = \{f(u_1, \ldots, u_n) \mid f \in K[x_1, \ldots, x_n]\}$$

3. $K[S] = \{f(s_1, \ldots, s_n) \mid n \in \mathbb{N},\ f \in K[x_1, \ldots, x_n],\ s_1, \ldots, s_n \in S\}$
4. $K(u) = \{f(u)g(u)^{-1} \mid f, g \in K[x],\ g(u) \neq 0\}$
5. $K(u_1, \ldots, u_n) = \{f(u_1, \ldots, u_n)g(u_1, \ldots, u_n)^{-1} \mid f, g \in K[x_1, \ldots, x_n],$ $g(u_1, \ldots, u_n) \neq 0\}$
6. $K(S) = \{f(s_1, \ldots, s_n)g(s_1, \ldots, s_n)^{-1} \mid n \in \mathbb{N},\ f, g \in K[x_1, \ldots, x_n],$ $s_1, \ldots, s_n \in S,\ g(s_1, \ldots, s_n) \neq 0\}$

Beweis: Wir beweisen nur 6., denn 3. funktioniert analog, und alle anderen Aussagen sind Spezialfälle von 3. oder 6.
Sei E die Menge auf der rechten Seite. Dann gilt jedenfalls offensichtlich $K \cup S \subseteq E$. Jeder Unterkörper von F, der $K \cup S$ enthält, muss E enthalten, da die Elemente von E nur durch

Summen, Produkte und Inversenbildung aus Elementen von $K \cup S$ gebildet werden. Also ist $E \subseteq K(S)$. Es muss nur noch gezeigt werden, dass E tatsächlich ein Körper ist:
$E \neq \emptyset$ und $E \setminus \{0\} \neq \emptyset$, weil $K \subseteq E$.
Seien $a, b \in E$, wobei $a = \frac{f(s_1,\ldots,s_n)}{g(s_1,\ldots,s_n)}$ und $b = \frac{h(t_1,\ldots,t_m)}{k(t_1,\ldots,t_m)}$ sei. Fasst man f, g, h, k als Polynome in $[x_1, \ldots, x_n, y_1, \ldots, y_m]$ auf, ergibt sich hiermit:

$$a - b = \frac{f(s_1, \ldots, t_m)}{g(s_1, \ldots, t_m)} - \frac{h(s_1, \ldots, t_m)}{k(s_1, \ldots, t_m)} = \frac{(fk - hg)(s_1, \ldots, t_m)}{(gk)(s_1, \ldots, t_m)}$$

und $(gk)(s_1, \ldots, t_m) = g(s_1, \ldots, s_n)k(t_1, \ldots, t_m) \neq 0$, also $a - b \in E$.
Wenn $b \neq 0$ ist, dann gilt außerdem:

$$ab^{-1} = \frac{f(s_1, \ldots, t_m)}{g(s_1, \ldots, t_m)} \cdot \frac{k(s_1, \ldots, t_m)}{h(s_1, \ldots, t_m)} = \frac{(fk)(s_1, \ldots, t_m)}{(gh)(s_1, \ldots, t_m)}$$

und $(gh)(s_1, \ldots, t_m) = g(s_1, \ldots, s_n)h(t_1, \ldots, t_m) \neq 0$, also $ab^{-1} \in E$.
Damit ist E ein Unterkörper von F, der $K \cup S$ enthält. ∎

Bemerkung: Sei $F : K$ eine Körpererweiterung und $u \in F$ algebraisch über K. Dann ist die Menge

$$\mathcal{N}_K(u) := \{f \in K[x] \mid f(u) = 0\} \neq \{0\}$$

ein Ideal von $K[x]$. Da $K[x]$ ein Hauptidealring ist, hat $\mathcal{N}_K(u)$ einen Erzeuger $m(x)$, d.h. $\mathcal{N}_K(u) = (m(x)) = m(x)K[x]$.

Da Erzeuger eines Ideals bis auf Multiplikation mit Einheiten eindeutig sind (Integritätsbereich), und Einheiten in $K[x]$ genau die Konstanten $\neq 0$ sind, folgt: Es gibt genau einen normierten Erzeuger von $\mathcal{N}_K(u)$.

Definition 18.9 Sei $F : K$ eine Körpererweiterung und $u \in F$ algebraisch über K. Der normierte Erzeuger des Ideals $\mathcal{N}_K(u) = \{f \in K[x] \mid f(u) = 0\}$ heißt *Minimalpolynom von u über K*. Das heißt, das Minimalpolynom von u ist jenes $m(x) \in K[x]$, sodass

$$\forall f \in K[x] : \ f(u) = 0 \iff \exists g \in K[x] : \ m(x) \cdot g(x) = f(x).$$

Definition 18.10 Eine Körpererweiterung $F : K$ heißt *einfach*, wenn es $u \in F$ gibt, sodass $F = K(u)$.

$F : K$ heißt *endlich erzeugt*, wenn es $u_1, \ldots, u_n \in F$ gibt, sodass $F = K(u_1, \ldots, u_n)$.

Proposition 18.11 Sei K ein Körper und $F = K(u)$ für $u \in F$, u transzendent über K (d.h. $F : K$ ist eine einfache transzendente Körpererweiterung). Dann ist $K(u) \simeq K(x)$ mittels eines Isomorphismus $\varphi : K(x) \to K(u)$ mit $\varphi(x) = u$ und $\varphi|_K = \mathrm{id}_K$.

Beweis: Sei $\psi : K[x] \to K(u)$ der Einsetzhomomorphismus mit $\psi(x) = u$ und $\psi|_K = \mathrm{id}$ (d.h. $\psi(f) = f(u)$ für $f \in K[x]$). Da $\psi(f) = f(u) \neq 0$ für alle $f \in K[x] \setminus \{0\}$ ist, also $\psi(f)$

für alle $f \in K[x] \setminus \{0\}$ invertierbar ist, kann ψ auf den Quotientenkörper $K(x)$ von $K[x]$ fortgesetzt werden: es gibt einen Homomorphismus $\overline{\psi} : K(x) \to K(u)$ mit $\overline{\psi}|_{K[x]} = \psi$.
Es gilt dann $\overline{\psi}|_K = \psi|_K = \mathrm{id}_K$ und $\overline{\psi}(x) = \psi(x) = u$, und wir wissen auch, wie $\overline{\psi}$ definiert ist: $\overline{\psi}(\frac{f}{g}) = \psi(f)\psi(g)^{-1} = f(u)g(u)^{-1}$
Man erhält $\operatorname{Im}\overline{\psi} = \{f(u)g(u)^{-1} \mid f, g \in K[x],\ g \neq 0\} = K(u)$ ($g \neq 0$ ist äquivalent zu $g(u) \neq 0$, weil u transzendent ist), d.h. $\overline{\psi}$ ist surjektiv. Weil zudem $\overline{\psi} \neq 0$ ist ($\overline{\psi}|_K = \mathrm{id}$, also jedenfalls $\overline{\psi} \neq 0$), muss nach dem vorigen Lemma $\overline{\psi}$ auch injektiv sein, d.h. $\overline{\psi}$ ist Isomorphismus, der zudem auch $\overline{\psi}(x) = u$ und $\overline{\psi}|_K = \mathrm{id}_K$ erfüllt. ∎

Satz 18.12 *Sei $F : K$ eine Körpererweiterung und $u \in F$ algebraisch über K, sodass $F = K(u)$ (d.h. $F : K$ ist eine einfache algebraische Körpererweiterung). Dann gilt:*

1. $K(u) = K[u]$
2. $K[u] \simeq {}^{K[x]}\!/_{m(x)}$ *, wobei $m(x)$ das Minimalpolynom von u über K ist*
3. $m(x)$ *ist irreduzibel*
4. $[K[u] : K] = \deg m$
5. $1, u, u^2, \ldots, u^{\deg m - 1}$ *ist eine Basis von $K[u]$ als K-Vektorraum.*

Beweis: Sei $\varphi : K[x] \to F$ der Einsetzhomomorphismus mit $\varphi(x) = u$, $\varphi \,|_K = \mathrm{incl}_{K \hookrightarrow F}$, das heißt $\varphi(f) = f(u)$. Dann gilt $\operatorname{Im}\varphi = \{f(u) \mid f \in K[x]\} = K[u]$ und ausserdem $\operatorname{Ker}\varphi = \{f \in K[x] \mid f(u) = 0\} = (m(x)) = m(x)K[x]$.

Nach dem 1.Isomorphiesatz gilt $K[u] = \operatorname{Im}\varphi \simeq {}^{K[x]}\!/_{(m(x))}$. Weil $K[u]$ als Unterring des Körpers F ein Integritätsbereich ist, ist $(m(x))$ ein Primideal von $K[x]$. Da $(m(x)) \neq \{0\}$ ist, muss $m(x)$ prim und daher auch irreduzibel sein. Somit ist $(m(x))$ maximal unter den Hauptidealen $\neq K[x]$, und weil $K[x]$ ein Hauptidealbereich ist, muss damit $(m(x))$ ein maximales Ideal sein. Daher ist ${}^{K[x]}\!/_{(m(x))} \simeq K[u]$ ein Körper, und es folgt weiters $K(u) = K[u]$.

$K(u) = K[u] = \{f(u) \mid f \in K[x]\}$, also hat jedes Element von $K(u)$ die Form $f(u)$ für ein $f \in K[x]$. Sei $f \in K[x]$ beliebig gewählt. Dann lässt es sich als $f(x) = q(x)m(x) + r(x)$ mit $r = 0$ oder $\deg r < \deg m =: n$ schreiben. Wendet man den Einsetzhomomorphismus an, ergibt sich $f(u) = q(u)m(u) + r(u) = r(u)$, also hat jedes $a \in K(u)$ die Form $a = r(u)$ mit einem $r = a_0 + \ldots + a_{n-1}x^{n-1}$. Damit ist $a = a_0 + \ldots + a_{n-1}u^{n-1}$, also erzeugt $\{1, \ldots, u^{n-1}\}$ $K(u)$ als Vektorraum über K.

Wenn andererseits $a_0 + \ldots + a_{n-1}u^{n-1} = 0$ ist, dann folgt $g \,|\, r = a_0 + \ldots + a_{n-1}x^{n-1}$, und weil $\deg r = n - 1 < \deg g$ ist, muss $r = 0$, also $a_i = 0\ \forall i$ sein. Also ist $\{1, \ldots, u^{n-1}\}$ linear unabhängig über K. ∎

Satz 18.13 (Adjunktion einer Nullstelle eines Polynoms) *Sei K ein Körper und $f \in K[x]$ mit $\deg f \geq 1$. Dann gilt:*

1. *Es existiert eine Körpererweiterung $F : K$ mit $F = K(u)$, sodass $f(u) = 0$ und $[K(u) : K] \leq \deg f$. Wenn f irreduzibel ist, dann gilt $[K(u) : K] = \deg f$.*

2. *Wenn f irreduzibel über K ist und $K(u)$, $K(v)$ einfache Erweiterungen von K mit $f(u) = 0$ und $f(v) = 0$, dann existiert ein Körperisomorphismus $\varphi : K(u) \to K(v)$ mit $\varphi(u) = v$ und $\varphi(k) = k$ für alle $k \in K$. Zudem gilt $[K(u) : K] = \deg f$.*

Beweis: Wir zeigen die Aussage für ein irreduzibles f (ansonsten kann man einen irreduziblen Faktor von f wählen und auf diesen den Rest des Beweises anwenden):

Weil f irreduzibel ist, ist (f) ein maximales Ideal in $K[x]$, daher ist $K[x]/(f)$ ein Körper. Sei $\pi : K[x] \to K[x]/(f)$ die kanonische Projektion. Dann ist $\pi|_K : K \to K[x]/(f)$ injektiv, da $\operatorname{Ker} \pi|_K = K \cap (f) = \{0\}$ ist.

Also ist K via $k \mapsto k + (f)$ eingebettet in $K[x]/(f) =: F$, d.h. $F : K$ ist eine Körpererweiterung. Sei ferner $u := x + (f) \in F$. Dann gilt:

$$f(u) = f(x) + (f) = f + (f) = (f) = 0 + (f) = 0_F$$

Also $f(u) = 0$. F wird von $u = x + (f) = \pi(x)$ erzeugt, da $K[x]$ von x erzeugt wird.

Weil f irreduzibel ist, ist f bis auf eine multiplikative Konstante Minimalpolynom von u über K, es gilt also $[K(u) : K] = \deg f$. Nach der Charakterisierung einfacher algebraischer Körpererweiterungen muss zudem $K(u) \simeq K[x]/(f) \simeq K(v)$ sein, wobei für den Isomorphismus $\varphi : K(u) \to K(v)$, der sich ergibt, offensichtlich $\varphi(u) = v$ und $\varphi(k) = k$ für alle $k \in K$ sein muss. ∎

Definition 18.14 Eine Körpererweiterung $F : K$ heißt *endlich-dimensional*, wenn $[F : K] = \dim_K F = n \in \mathbb{N}$ endlich ist.

Proposition 18.15 Ist eine Körpererweiterung $F : K$ endlich-dimensional, dann ist sie endlich-erzeugt und algebraisch.

Beweis: Sei $[F : K] = n$, für jedes $u \in K$ sind dann 1, u, u^2, …, u^n K-linear abhängig, d.h. es gibt $a_0, \ldots, a_n$, die nicht alle gleich 0 sind, sodass $a_0 + a_1 u + \ldots + a_n u^n = 0$. Somit $existsf \in K[x]$, $f \neq 0$, $\deg f \leq n$, sodass $f(u) = 0$ und u ist algebraisch.

Sei $u_1 \in F \setminus K$, dann setze $K_1 = K[u_1] = K(u_1)$ (adjungiere u_1 zu K). Dann gilt für die Grade, dass $[F : K] = [F : K_1][K_1 : K]$. Da $K_1 \neq K$, gilt $[K_1 : K] > 1$ und daher $[F : K_1] < [F : K]$. Durch Iteration erhalten wir zu jedem $K_i \neq F$ durch Adjunktion eines Elements $u_{i+1} \in F \setminus K_i$ einen Körper $K_{i+1} = K_i[u_{i+1}] = K[u_1, \ldots, u_{i+1}]$, für den $[F : K_{i+1}] < [F : K_i]$ gilt. Diese Prozedur bricht nach endlich vielen ($\leq \log_2(n)$) Schritten ab mit $F = K_i = K[u_1, \ldots, u_i]$. ∎

Proposition 18.16 Sei $F : K$ eine Körpererweiterung, wobei $F = K(s_1, \ldots, s_n)$, und alle s_i algebraisch über K sind. Dann ist $F : K$ endlich-dimensional.

Beweis: Das Element s_i ist algebraisch über K, also auch über $K(s_1, \ldots, s_{i-1})$. Deswegen gilt $K(s_1, \ldots, s_i) = K(s_1, \ldots, s_{i-1})(s_i) = K(s_1, \ldots, s_{i-1})[s_i]$, und $[K(s_1, \ldots, s_{i-1})[s_i] : K(s_1, \ldots, s_{i-1})] =: m_i$ ist endlich. Es folgt:

$$\begin{aligned}[F : K] &= [K(s_1, \ldots, s_n) : K] \\ &= [K(s_1, \ldots, s_n) : K(s_1, \ldots, s_{n-1})] \ldots [K(s_1) : K] \\ &= m_n \ldots m_1\end{aligned}$$

Damit ist $[F : K]$ endlich. ∎

Proposition 18.17 Eine Körpererweiterung $F : K$ ist genau dann endlich-dimensional, wenn $F : K$ endlich-erzeugt und algebraisch ist.

Beweis: Folgerung aus den vorigen Propositionen. ∎

Bemerkung: Sei K ein Körper. Ein Ring A heißt K-*Algebra*, wenn A ein K-Vektorraum ist, und

$$\forall a, b \in A,\ k \in K :\ k(ab) = (ka)b = a(kb).$$

Man kann Elemente von A in Polynome aus $K[x]$ einsetzen und analog zu Körpererweiterungen algebraische Elemente definieren. Diese haben Minimalpolynome (das sind normierte Erzeuger der Ideale $\{f \in K[x] \mid f(a) = 0\}$). Solche Minimalpolynome müssen nicht irreduzibel sein.

Beispiel: $A = M_n(K)$ ist eine K-Algebra. Das Minimalpolynom von $C \in M_n(K)$ bekommt man durch Diagonalisierung von $xI - C \in M_n(K[x])$ mittels elementarer Zeilen- und Spaltenumformungen. Das Minimalpolynom ist der invariante Faktor, der von allen anderen geteilt wird.

Das Produkt der invarianten Faktoren von $xI - C$ ist χ_C, das Charakteristische Polynom von C. Es gilt $\chi_C = \det(xI - C)$, da sich die Determinante unter elementaren Zeilen- und Spaltenumformungen nicht verändert.

19 Charakteristik

Definition 19.1 Sei R ein Ring. Dann heißt

$$\mathrm{Ann}_{\mathbb{Z}}(R) = \{n \in \mathbb{Z} \mid \forall r \in R : \ nr = 0\}$$

der *Annihilator* von R.

Bemerkung: $\mathrm{Ann}_{\mathbb{Z}}(R)$ ist eine Untergruppe von $(\mathbb{Z}, +)$, somit $\exists n \in \mathbb{N} : \ \mathrm{Ann}_{\mathbb{Z}}(R) = n\mathbb{Z}$.

Definition 19.2 Jenes $n \in \mathbb{N}$, sodass $\mathrm{Ann}_{\mathbb{Z}}(R) = n\mathbb{Z}$, heißt *Charakteristik* $\chi(R)$ von R. Wenn $\mathrm{Ann}_{\mathbb{Z}}(R) \neq \{0\}$, dann gilt

$$\chi(R) = \min\{n \in \mathbb{N} \mid \forall r \in R : \ nr = 0\} \quad (= \min(n\mathbb{Z} \cap \mathbb{N}) \ )$$

Proposition 19.3 Wenn R ein Ring mit Eins ist und $\{n \in \mathbb{N} \,|\, n1_R = 0_R\} = \emptyset$, dann ist $\chi(R) = 0$ andernfalls ist $\chi(R) = \min\{n \in \mathbb{N} \,|\, n1_R = 0_R\}$.

Beweis: als Übung. ∎

Proposition 19.4 Sei R ein Integritätsbereich, dann ist $\chi(R) = 0$ oder $\chi(R) = p$ eine Primzahl.

Beweis: Angenommen, $\chi(R)$ wäre weder 0 noch eine Primzahl. Dann ist $\chi(R) = nm$ für $n, m \in \mathbb{N}$, $n, m > 1$.

Es gilt $\chi(R) = \min\{k \in \mathbb{N} \,|\, \forall r \in R \ kr = 0\}$. Aus $m > 1$ folgt $n < nm = \chi(R)$, daher gibt es ein $r \in R$, sodass $nr \neq 0$ ist, und ebenso ein $s \in R$, sodass $ms \neq 0$ ist. Es gilt jedoch $(nr)(ms) = (nm)(rs) = \chi(R)(rs) = 0$, also müsste R Nullteiler haben, ein Widerspruch. ∎

Bemerkung: Insbesondere haben Körper immer Charakteristik 0 oder p prim.

Beispiel: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sind Körper mit Charakteristik 0.

$\mathbb{Z}_p = {}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$ (p prim) ist ein Körper der Charakteristik p. Es gibt aber noch weitere Körper der Charakteristik p. Z.B. gibt es für jede Potenz $q = p^n$ genau einen endlichen Körper der Ordnung q. Dieser hat Charakteristik p.

Definition 19.5 Sei R ein Ring mit Eins. Der von 1 erzeugte Unterring von R heißt *Primring* von R, $\Pi_R := \bigcap_{S \leq R, 1 \in S} S$.

Sei K ein Körper. Der von 1 erzeugte Unterkörper von K heißt *Primkörper* von K.

Bemerkung: Wenn $\chi(R) = 0$, dann ist der Primring von R isomorph zu $\mathbb{Z}$ (Wenn R auch ein Körper ist, dann ist sein Primkörper isomorph zu $\mathbb{Q}$). Wenn $\chi(R) = n$, dann ist der Primring isomorph zu $\mathbb{Z}_n$. Sei K ein Körper mit $\chi(K) = p$, dann ist der Primring von K gleich dem Primkörper von K isomorph zu $\mathbb{Z}_p$.

BEMERKUNG: Jeder endliche Körper hat p^n Elemente für ein $p \in \mathbb{P}$, $n \in \mathbb{N}$: Aus K endlich folgt $\chi(K) = p$ prim (wäre $\chi(K) = 0$, dann wäre $\mathbb{Q}$ isomorph zu einem Teilkörper von K und daher endlich). Somit ist der Primring von K isomorph zu $\mathbb{Z}_p$. K ist also ein $\mathbb{Z}_p$-Vektorraum von endlicher Dimension n und es folgt $|K| = p^n$.

BEMERKUNG: Für jede Primzahlpotenz q gibt es (bis auf Isomorphie) genau einen endlichen Körper der Ordnung q.

Index