KAPITEL 7

Ringe

1. Definition und Beispiele

DEFINITION. *Ein* **Ring** R *ist eine Menge mit zwei Verknüpfungen* $+$ *und* $\cdot$*, die* **Addition** *und* **Multiplikation** *genannt werden, wobei folgende Eigenschaften erfüllt sind:*

(1) $(R,+)$ *ist eine abelsche Gruppe. Explizit:*
   (a) *Es gilt das Assoziativgesetz:* $a+(b+c)=(a+b)+c$ *für alle* $a,b,c\in R$.
   (b) *Es gibt ein neutrales Element* 0 *(Null):* $a+0=0+a=a$ *für alle* $a\in R$.
   (c) *Zu jedem* $a\in R$ *gibt es ein inverses Element* $-a$*:* $a+(-a)=(-a)+a=0$.
   (d) *Es gilt das Kommutativgesetz:* $a+b=b+a$ *für alle* $a,b\in R$.

(2) $(R,\cdot)$ *ist ein Monoid. (Statt* $a\cdot b$ *wird oft einfach* ab *geschrieben.) Explizit:*
   (a) *Es gilt das Assoziativgesetz:* $a(bc)=(ab)c$ *für alle* $a,b,c\in R$.
   (b) *Es gibt ein neutrales Element* 1 *(Eins):* $a\cdot 1=1\cdot a=a$ *für alle* $a\in R$.
   (c) *Eine* **Einheit** a *von* R *ist ein bzgl.* $\cdot$ *invertierbares Element. Das zu* a *inverse Element wird als* a^{-1} *geschrieben:* $a\cdot a^{-1}=a^{-1}\cdot a=1$.
   (d) *Die Einheiten von* R *bilden bzgl. der Multiplikation eine Gruppe, die als* **Einheitengruppe** *bezeichnet und als* R^* *geschrieben wird:* $R^*=\{a\in R: \text{es gibt ein } b\in R \text{ mit } ab=ba=1\}$.
   (e) *Ist die Multiplikation kommutativ, d.h.* $ab=ba$ *für alle* $a,b\in R$*, so spricht man von einem* **kommutativen Ring**.

(3) *Es gelten die Distributivgesetze:*

$$a(b+c)=ab+ac \quad \text{und} \quad (a+b)c=ac+bc \quad \text{für alle } a,b,c\in R.$$

Dabei wird die Konvention „Punkt vor Strich“ verwendet.

Beispiele:

(1) Die ganzen Zahlen $\mathbb{Z}$ bilden mit der üblichen Addition und Multiplikation einen Ring. Die Einheitengruppe ist $\mathbb{Z}^*=\{\pm 1\}$.

(2) Die Körper $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sind Ringe. Die Einheitengruppen sind $\mathbb{Q}^*=\mathbb{Q}\setminus\{0\}$, $\mathbb{R}^*=\mathbb{R}\setminus\{0\}$, $\mathbb{C}^*=\mathbb{C}\setminus\{0\}$.

(3) Ist K ein Körper und $n\in\mathbb{N}$, so bilden die quadratischen $n\times n$-Matrizen

$$\mathrm{M}_n(K)=\left\{\begin{pmatrix} a_{11} & \dots & a_{1n}\\ \vdots & & \vdots\\ a_{n1} & \dots & a_{nn}\end{pmatrix} : a_{ij}\in K \text{ für alle } i,j\right\}$$

mit der üblichen Matrizenaddition und Matrizenmultiplikation einen Ring. Das neutrale Element der Addition ist die Nullmatrix 0, das neutrale Element der Multiplikation die Einheitsmatrix:

$$0=\begin{pmatrix} 0 & \dots & 0\\ \vdots & & \vdots\\ 0 & \dots & 0\end{pmatrix} \quad 1=\begin{pmatrix} 1 & \dots & 0\\ \vdots & & \vdots\\ 0 & \dots & 1\end{pmatrix}.$$

Die Einheitengruppe ist

$$\mathrm{M}_n(K)^*=\mathrm{GL}_n(K)=\{A\in\mathrm{M}_n(K):\det(A)\neq 0\}.$$

Datei: alg_ringe.tex. Version vom 8.1.2024

(4) Definiert man auf der einelementigen Menge $R = \{a\}$ Addition und Multiplikation durch $a+a = a$ und $a \cdot a = a$, so erhält man einen Ring mit $a = 0 = 1$. Natürlich gilt dann auch $R^* = R$. Diesen Ring nennt man auch den **Nullring**.

Bemerkungen:

(1) In dieser Vorlesung ist ein Ring bezüglich der Multiplikation ein Monoid, ein Ring besitzt also immer eine Eins. Diese Konvention wird auch in den Algebra-Büchern von Bosch, Bourbaki, Jacobson, Lang, Shafarevich verwendet.
(2) Fordert man in der Definition eines Rings nicht, dass R bezüglich der Multiplikation ein Monoid ist, sondern nur, dass das Assoziativgesetz gilt, so erhält man einen „Ring ohne Eins“, der bei Bourbaki Pseudo-Ring (französich: pseudo-anneau, englisch: pseudo-ring) genannt wird.
(3) Triviale Beispiele von Pseudo-Ringen erhält man, wenn man eine abelsche Gruppe $(R, +)$ hernimmt und die Multiplikation durch $a \cdot b = 0$ für alle $a, b \in R$ definiert.
(4) In manchen Algebra-Büchern wird ein Pseudo-Ring auch Ring genannt, ein Ring dann „Ring mit 1“ (Fischer, Wüstholz/Fuchs) oder „unitärer Ring“ (Wüstholz/Fuchs).

LEMMA. *Sei R ein Ring. Dann gilt für alle $x, y \in R$:*

(1) $0 \cdot x = x \cdot 0 = 0$.
(2) $(-x) \cdot y = x \cdot (-y) = -xy$.
(3) $(-x)(-y) = xy$.
(4) $(-1) \cdot x = x \cdot (-1) = -x$.

Beweis:

(1) Es ist $0x = (0 + 0)x = 0x + 0x$, also $0x = 0$. Genauso folgt $x0 = 0$.
(2) $xy + (-x)y = (x + (-x))y = 0y \overset{(1)}{=} 0$, also $(-x)y = -xy$.
(3) $(-x)(-y) = -x(-y) = -(-xy) = xy$ unter Verwendung von (2).
(4) $(-1) \cdot x = -(1 \cdot x) = -x$ unter Verwendung von (2). ■

Bemerkungen: Sei R ein Ring.

(1) Ist $a \in R$, so ist $-a$ das zu a inverse Element bzgl. der Addition: $a + (-a) = (-a) + a = 0$. Statt $b + (-a)$ schreibt man auch $b - a$:

$$b - a = b + (-a).$$

(2) Dann gilt natürlich auch hier das Distributivgesetzt

$$a(b - c) = ab - ac \quad \text{und} \quad (a - b)c = ac - bc.$$

(3) Es gilt auch das allgemeine Distributivgesetz, das man leicht durch Induktion beweist:

$$\sum_{i=1}^{m} a_i \cdot \sum_{j=1}^{m} b_j = \sum_{i=1}^{m} \sum_{j=1}^{n} a_i b_j.$$

LEMMA. *Sei R ein Ring.*

(1) *Gilt in R die Gleichheit $1 = 0$, so ist $R = \{0\}$, also der Nullring, und $R^* = R$.*
(2) *Ist R nicht der Nullring, so ist $1 \neq 0$ und*

$$R^* \subseteq R \setminus \{0\}.$$

Beweis:

(1) Gilt in R die Gleichheit $1 = 0$, so gilt für alle $x \in R$ die Gleichung $x = 1 \cdot x = 0 \cdot x = 0$, also $R = \{0\}$.
(2) Ist R nicht der Nullring, so ist $1 \neq 0$. Da für alle $a \in R$ gilt $a \cdot 0 = 0 \cdot a = 0 \neq 1$ ist 0 nicht invertierbar, d.h. $R^* \subseteq R \setminus \{0\}$. ■

SATZ. *Für $n \in \mathbb{N}$ ist $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ mit $+_{\bmod n}$ als Addition und $\cdot_{\bmod n}$ als Multiplikation ein kommutativer Ring (mit n Elementen):*

$$a +_{\bmod n} b = (a+b) \bmod n, \quad a \cdot_{\bmod n} b = (ab) \bmod n.$$

Die Einheitengruppe ist

$$\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n : \mathrm{ggT}(n,a) = 1\} \text{ mit } |\mathbb{Z}_n^*| = \varphi(n).$$

Beweis: Wir müssen nur noch ein Distributivgesetz überprüfen, da das zweite dann mit der Kommutativität der Multiplikation folgt. Es ist

$$\begin{aligned} a \cdot_{\bmod n} (b +_{\bmod n} c) &= a \cdot_{\bmod n} \Big((b+c) \bmod n\Big) = \Big(a \cdot \Big((b+c) \bmod n\Big)\Big) \bmod n = \\ &= \left(a \cdot \left(b + c - \left\lfloor \frac{b+c}{n} \right\rfloor n\right)\right) \bmod n = \\ &= \left(ab + ac - a \left\lfloor \frac{b+c}{n} \right\rfloor n\right) \bmod n = (ab+ac) \bmod n. \end{aligned}$$

Andererseits gilt

$$\begin{aligned} (a \cdot_{\bmod n} b) +_{\bmod n} (a \cdot_{\bmod n} c) &= (ab \bmod n) +_{\bmod n} (ac \bmod n) = \\ &= \left(ab - \left\lfloor \frac{ab}{n} \right\rfloor n\right) +_{\bmod n} \left(ac - \left\lfloor \frac{ac}{n} \right\rfloor n\right) = \\ &= \left(ab - \left\lfloor \frac{ab}{n} \right\rfloor n + ac - \left\lfloor \frac{ac}{n} \right\rfloor n\right) \bmod n = \\ &= (ab+ac) \bmod n. \end{aligned}$$

Damit folgt

$$a \cdot_{\bmod n} (b +_{\bmod n} c) = (a \cdot_{\bmod n} b) +_{\bmod n} (a \cdot_{\bmod n} c),$$

was zu zeigen war. ■

Bemerkung: Wir betrachten den Ring $\mathbb{Z}_n$. Für $a \in \mathbb{Z}_n$ ist $-a$ das zu a bzgl. der Addition inverse Element. Auf diese Weise können wir -1 als Element des Rings $\mathbb{Z}_n$ betrachten. Dann ist

$$-1 = n - 1.$$

Da wir in $\mathbb{Z}_n$ Summen bilden können, können wir auch analog für $k \in \mathbb{Z}$ wegen

$$k = \begin{cases} \sum_{i=1}^{k} 1 & \text{für } k \geq 1, \\ 0 & \text{für } k = 0, \\ \sum_{i=1}^{|k|} (-1) & \text{für } k \leq -1 \end{cases}$$

k als Element von $\mathbb{Z}_n$ betrachten. Es gilt dann

$$k = (k \bmod n) \text{ in } \mathbb{Z}_n.$$

Das Produkt von Ringen ist wieder ein Ring:

SATZ. *Ist $(R_i)_{i \in I}$ eine Familie von Ringen, so wird das* **Produkt**

$$\prod_{i \in I} R_i = \{(a_i) : a_i \in R_i\}$$

durch

$$(a_i) + (b_i) = (a_i + b_i), \quad (a_i) \cdot (b_i) = (a_i \cdot b_i)$$

zu einem Ring mit Null $(0)_{i \in I}$ und Eins $(1)_{i \in I}$. Es ist

$$\left(\prod_{i \in I} R_i\right)^* = \{(a_i)_i \in I : a_i \in R_i^*\} = \prod_{i \in I} R_i^*.$$

Beispiel:

$$\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0),(0,1),(1,0),(1,1)\}.$$

Durch Produktbildung kann man sich also leicht weitere Beispiele von Ringen verschaffen.

DEFINITION. *Sei R ein Ring.*

(1) *Ein* **Schiefkörper** *(oder auch* **Divisionsring***) ist ein Ring R, für den gilt*

$$R^* = R \setminus \{0\}.$$

Anders ausgedrückt: In R ist $1 \neq 0$ und jedes von 0 verschiedene Element ist invertierbar.

(2) *Ein* **Körper** *ist ein kommutativer Ring K, für den gilt*

$$K^* = K \setminus \{0\}.$$

Anders ausgedrückt: In K gilt $1 \neq 0$, die Multiplikation ist kommutativ und jedes von 0 verschiedene Element ist invertierbar.

Beispiele:

(1) $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$ sind Körper.
(2) Ist p eine Primzahl, so ist $\mathbb{Z}_p^* = \{a \in \mathbb{Z}_p : \mathrm{ggT}(p,a) = 1\} = \{1,\ldots,p\} = \mathbb{Z}_p \setminus \{0\}$, also ist $\mathbb{Z}_p$ ein Körper (mit p Elementen). Man findet dafür auch die Schreibweise $\mathbb{F}_p$, da im Englischen „endlicher Körper“ „finite field“ heißt.
(3) In den Aufgaben wird der nichtkommutative Schiefkörper der **Hamiltonschen Quaternionen** eingeführt.

DEFINITION. *Ein Ring R heißt* **Integritätsring** *(oder* **Integritätsbereich***), wenn R kommutativ ist, $1 \neq 0$ gilt und für $x, y \in R$ gilt:*

$$xy = 0 \quad \Longrightarrow \quad x = 0 \text{ oder } y = 0.$$

Die letzte Bedingung lässt sich auch so formulieren:

$$x \neq 0 \text{ und } y \neq 0 \quad \Longrightarrow \quad xy \neq 0,$$

oder in Worten: „Ein Produkt ist genau dann 0, wenn einer der Faktoren 0 ist“. (Man sagt auch, R ist nullteilerfrei.)

Beispiele:

(1) $\mathbb{Z}$ ist ein Integritätsring.
(2) Körper K sind Integritätsringe:

$$\mathbb{Q}, \quad \mathbb{R}, \quad \mathbb{C}, \quad \mathbb{Z}_p \text{ für eine Primzahl } p.$$

(Denn sind $x, y \in K$ mit $xy = 0$ und $x \neq 0$, so folgt $y = (x^{-1}x)y = x^{-1}(xy) = 0$.)

(3) Ist $n \in \mathbb{N}$ keine Primzahl, so ist $\mathbb{Z}_n$ kein Integritätsring: Im Fall $n = 1$ ist $\mathbb{Z}_n$ der Nullring, also $1 = 0$, im Fall $n > 1$ ist n zusammengesetzt, d.h. es gibt $a, b \in \mathbb{N}$ mit $1 < a, b < n$ und $ab = n$; in $\mathbb{Z}_n$ gilt dann $ab = 0$.

Bemerkung: Die Bezeichnung *Integritätsring* wird in den Algebra-Büchern von Bosch und Fischer verwendet. Im Buch von Wüstholz/Fuchs steht *Integritätsbereich*. Lang spricht von *entire ring* und ist mit der auch verwendeten Bezeichnung *integral domain* nicht ganz glücklich.

2. Unterringe

DEFINITION. *Ist R ein Ring, so nennt man eine Teilmenge $S \subseteq R$ einen* **Unterring** *von R, falls S mit der Addition und der Multiplikation von R einen Ring bildet und die Eins von R in S enthalten ist. (Man nennt dann R auch einen* **Oberring** *von S.)*

LEMMA (Kriterium für einen Unterring). *Sei R ein Ring. Eine Teilmenge $S \subseteq R$ ist genau dann ein Unterring von R, wenn folgende Bedingungen erfüllt sind:*

(1) $0 \in S$,
(2) $x, y \in S \Longrightarrow x + y \in S$,
(3) $x \in S \Longrightarrow -x \in S$,
(4) $1 \in S$,
(5) $x, y \in S \Longrightarrow xy \in S$.

(Dann ist S selbst ein Ring.)

Beispiele:

(1) $\mathbb{Z}$ ist ein Unterring von $\mathbb{Q}$, $\mathbb{Q}$ ist ein Unterring von $\mathbb{R}$, $\mathbb{R}$ ist ein Unterring von $\mathbb{C}$.
(2) Der einzige Unterring von $\mathbb{Z}$ ist $\mathbb{Z}$ selbst.
(3) Im Matrizenring $\mathrm{M}_2(\mathbb{C})$ sei
$$\mathbb{H} = \left\{ \begin{pmatrix} x & y \\ -\overline{y} & \overline{x} \end{pmatrix} : x, y \in \mathbb{C} \right\},$$
wobei $\overline{\ }$ für die komplexe Konjugation steht. In den Aufgaben wird gezeigt, dass $\mathbb{H}$ ein (nicht-kommutativer) Schiefkörper ist. (Man nennt $\mathbb{H}$ auch den **Schiefkörper der Hamiltonschen Quaternionen**.)
(4) Unterringe eines Integritätsrings sind wieder Integritätsringe.

DEFINITION. *Ist R ein Ring, so heißt*
$$Z(R) = \{x \in R : xy = yx \text{ für alle } y \in R\}$$
das **Zentrum** *von R.*

LEMMA. *Für einen Ring R ist das Zentrum $Z(R)$ ein kommutativer Unterring von R. (Ist R kommutativ, so gilt natürlich $Z(R) = R$.)*

LEMMA. *Sei R ein Ring.*

(1) *Ist $R_i, i \in I$, eine Familie von Unterringen von R, so ist auch der Durchschnitt*
$$\bigcap_{i \in I} R_i$$
ein Unterring von R.
(2) *Ist $X \subseteq R$ eine beliebige Teilmenge von R, so ist*
$$\bigcap_{\substack{S \text{ Unterring von } R \\ X \subseteq S}} S$$
der kleinste Unterring von R, der X enthält. (Man nennt ihn auch den von X **erzeugten Unterring** *von R.)*

Mit dem Lemma kann man nun Folgendes definieren:

DEFINITION. *Sei S ein Ring und R ein Unterring von S.*

(1) *Ist M eine Teilmenge von S, so schreibt man $R[M]$ für den kleinsten Unterring von S, der R und M enthält.*

(2) *Ist* $M = \{\alpha_1, \ldots, \alpha_n\}$*, so schreibt man statt* $R[\{\alpha_1, \ldots, \alpha_n\}]$ *auch kurz*

$$R[\alpha_1, \ldots, \alpha_n].$$

(Man benutzt für $R[\alpha]$ *auch die Sprechweise „*R *adjungiert* α*“.)*

Beispiel: In $\mathbb{C}$ betrachten wir den Unterring $\mathbb{Z}$ und das Element i. Da für $a, b, c, d \in \mathbb{Z}$ gilt

$$(a + bi) + (c + di) = (a + c) + (b + d)i \quad \text{und} \quad (a + bi)(c + di) = (ac - bd) + (ad + bc)i,$$

sieht man schnell, dass

$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$$

gilt.

Manchmal kann man sofort eine Beschreibung von $R[\alpha]$ angeben:

LEMMA. *Ist* S *ein kommutativer Ring,* $R \subseteq S$ *ein Unterring und* $\alpha \in S$*, so ist*

$$R[\alpha] = \{a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n : n \in \mathbb{N}, a_0, a_1, \ldots, a_n \in R\}.$$

Beweis: Ist $\widetilde{R} \subseteq S$ ein Ring, der R und α enthält, so gilt natürlich auch

$$\{a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n : n \in \mathbb{N}, a_0, a_1, \ldots, a_n \in R\} \subseteq \widetilde{R}.$$

Da die linke Seite aber ein Unterring von S ist, ist die linke Seite der kleinste Unterring, der R und α enthält, woraus die Behauptung folgt. ■

3. Polynome in einer Veränderlichen/Unbestimmten über einem kommutativen Ring R

Es gibt verschiedene Möglichkeiten, Polynome einzuführen. Wir beginnen mit einer Variante, die auch van der Waerden in seinem Algebra-Buch benutzt.

Polynome in einer Veränderlichen/Unbestimmten über einem kommutativen Ring R:

(1) Ein **Polynom** f in einer Unbestimmten x mit Koeffizienten aus einem kommutativen Ring R ist eine endliche Summe

$$f = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \text{ mit } a_0, a_1, a_2, \ldots, a_n \in R.$$

Statt a_0 schreibt man auch a_0x^0. Man kann auch künstlich Summanden $0 \cdot x^i$ anhängen. Dann kann man auch schreiben

$$f = a_0 + a_1x + a_2x^2 + \cdots = \sum_{i \geq 0} a_ix^i,$$

wobei aber $a_i = 0$ ab einem bestimmten Index i_0 gilt. (Hier steht also keine unendliche Summe, wie man sie aus der Analysis kennt.) Die Zahlen a_i eines Polynoms $f = \sum_{i \geq 0} a_ix^i$ nennt man die **Koeffizienten** des Polynoms, a_i den Koeffizienten bei x^i. Sind alle Koeffizienten 0, spricht man vom **Nullpolynom**:

$$0 = 0 + 0 \cdot x + 0 \cdot x^2 + 0 \cdot x^3 + \ldots$$

Ist $f = \sum_{i \geq 0} a_ix^i$ nicht das Nullpolynom, so kann man schreiben

$$f = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \text{ mit } a_n \neq 0.$$

Man nennt n den **Grad** des Polynoms f und schreibt $\operatorname{grad}(f) = n$. Den Term a_nx^n nennt man den **Leitterm** von f, a_n wird auch **Leitkoeffizient** genannt. Ist $a_n = 1$, so nennt man das Polynom **normiert**. Den Grad des Nullpolynoms definieren wir als $-\infty$, also $\operatorname{grad}(0) = -\infty$.

(2) Zwei Polynome $f = \sum_{i \geq 0} a_ix^i$ und $g = \sum_{i \geq 0} b_ix^i$ definiert man als gleich, wenn alle entsprechenden Koeffizienten gleich sind, d.h.

$$\sum_{i \geq 0} a_ix^i = \sum_{i \geq 0} b_ix^i \quad \Longleftrightarrow \quad a_i = b_i \text{ für alle } i \geq 0.$$

Diese Eigenschaft läuft auch unter der Bezeichnung **Koeffizientenvergleich**.

(3) Polynome kann man addieren:

$$\sum_{i\geq 0} a_i x^i + \sum_{i\geq 0} b_i x^i = \sum_{i\geq 0} (a_i + b_i) x^i$$

und multiplizieren:

$$\sum_{i\geq 0} a_i x^i \cdot \sum_{i\geq 0} b_i x^i = \sum_{i\geq 0} \left(\sum_{j+k=i} a_j b_k \right) x^i.$$

Die Multiplikation ist so gemacht, dass gilt

$$\sum_{i\geq 0} a_i x^i \cdot \sum_{i\geq 0} b_i x^i = \sum_{i\geq 0} a_i x^i \cdot \sum_{j\geq 0} b_j x^j = \sum_{i\geq 0} \sum_{j\geq 0} a_i b_j x^{i+j} = \sum_{k\geq 0} \left(\sum_{\substack{i\geq 0 \\ j\geq 0 \\ i+j=k}} a_i b_j \right) x^k.$$

Wir schreiben dies nochmals aus:

$$\begin{aligned} & (a_0 + a_1 x + \cdots + a_m x^m)(b_0 + b_1 x + \cdots + b_n x^n) = \\ = \; & a_0 b_0 + (a_0 b_1 + a_1 b_0) x + (a_0 b_2 + a_1 b_1 + a_2 b_0) x^2 + \dots \\ & \dots \\ & + (a_{m-1} b_n + a_m b_{n-1}) x^{m+n-1} + a_m b_n x^{m+n}. \end{aligned}$$

(4) Die Menge dieser Polynome schreibt man als $R[x]$:

$$R[x] = \{ \sum_{i\geq 0} a_i x^i : a_i \in R, a_i \neq 0 \text{ für nur endlich viele } i \in \mathbb{N}_0 \}.$$

Durch obige Definition wird $R[x]$ zu einem kommutativen Ring, dem **Polynomring in der Unbestimmten x über R.**

(5) Wir fassen R als Unterring von $R[x]$ auf, wobei die Elemente von R den konstanten Polynomen (Polynomen vom Grad 0) entsprechen.

(6) In Polynome kann man **einsetzen**: Ist S ein Oberring von R und $a \in S$, ist $f = a_0 + a_1 x + a_2 x^2 + \dots$, so definiert man

$$f(a) = a_0 + a_1 a + a_2 a^2 + \dots$$

Nach Definition der Addition und Multiplikation von Polynomen ist dann klar, dass folgende Beziehungen gelten:

$$f(x) + g(x) = h(x) \quad \Longrightarrow \quad f(a) + g(a) = h(a)$$

und

$$f(x) g(x) = h(x) \quad \Longrightarrow \quad f(a) g(a) = h(a).$$

Bemerkung: Man kann den Polynomring $R[x]$ auch etwas formaler einführen:

(1) Sei R ein kommutativer Ring. Dann betrachten wir

$$\widetilde{R} = \{ (a_i)_{i\geq 0} : a_i \in R, a_i = 0 \text{ für fast alle } i \}.$$

Durch komponentenweise Addition erhalten wir eine Addition auf dieser Menge:

$$(a_i) + (b_i) = (c_i) \text{ mit } c_i = a_i + b_i.$$

Die Multiplikation wird definiert durch

$$(a_i) \cdot (b_i) = (c_i) \text{ mit } c_i = \sum_{j+k=i} a_j b_k.$$

Dann zeigt man, dass $\widetilde{R}$ ein kommutativer Ring ist. Die Eins ist $(1, 0, 0, 0, \dots)$.

(2) Mit der Identifikation

$$a \leftrightarrow (a, 0, 0, 0, \dots) \quad \text{für} \quad a \in R$$

kann man R als Unterring von $\widetilde{R}$ auffassen.

(3) Definiert man

$$x = (0, 1, 0, 0, 0, \dots),$$

so ist für $a \in R$ und $i \in \mathbb{N}_0$

$$ax^i = (0, 0, 0, \dots, 0, a, 0, 0, 0, \dots) \text{ mit } a \text{ an der Stelle } i.$$

Es folgt dann

$$(a_0, a_1, a_2, \dots) = \sum_{i \geq 0} a_i x^i.$$

Damit erhält man eine Bijektion

$$\widetilde{R} \leftrightarrow R[x].$$

Beispiel: Wir rechnen in $\mathbb{Z}_6[x]$:

$$(2 + 3x)(3 + 2x) = 2 \cdot 3 + 2 \cdot 2x + 3x \cdot 3 + 3x \cdot 2x = 0 + 4x + 3x + 0 = x.$$

LEMMA. *Ist $R[x]$ der Polynomring in der Unbestimmten x über dem kommutativen Ring R, so gilt für $f, g \in R[x]$:*

(1) $\operatorname{grad}(f + g) \leq \max(\operatorname{grad}(f), \operatorname{grad}(g))$.
(2) $\operatorname{grad}(fg) \leq \operatorname{grad}(f) + \operatorname{grad}(g)$.
(3) *Ist f oder g normiert, so gilt* $\operatorname{grad}(fg) = \operatorname{grad}(f) + \operatorname{grad}(g)$.
(4) *Ist R ein Integritätsring, so gilt* $\operatorname{grad}(fg) = \operatorname{grad}(f) + \operatorname{grad}(g)$.

Beweis: Ist eines der Polynome f, g das Nullpolynom, so gelten die Formeln des Lemmas trivialerweise wegen $\operatorname{grad}(0) = -\infty$. Wir können also $f, g \neq 0$ voraussetzen und schreiben

$$f = a_0 + a_1 x + a_2 x^2 + \cdots + a_m x^m \text{ mit } a_m \neq 0 \quad \text{und} \quad g = b_0 + b_1 x + b_2 x^2 + \cdots + b_n x^n \text{ mit } b_n \neq 0.$$

(1) Wir können o.E. $m \geq n$ annehmen. Dann ist

$$f + g = (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_n + b_n)x^n + a_{n+1}x^{n+1} + \cdots + a_m x^m.$$

Dann folgt $\operatorname{grad}(f + g) \leq \max(\operatorname{grad}(f), \operatorname{grad}(g))$. Man sieht auch:

$$\operatorname{grad}(f) \neq \operatorname{grad}(g) \quad \Longrightarrow \quad \operatorname{grad}(f + g) = \max(\operatorname{grad}(f), \operatorname{grad}(g)).$$

(2-4) Es ist

$$fg = a_0 b_0 + (a_0 b_1 + a_1 b_0)x + \cdots + (a_{m-1} b_n + a_m b_{n-1})x^{m+n-1} + a_m b_n x^{m+n}.$$

- Aus der Darstellung folgt sofort $\operatorname{grad}(fg) \leq m + n = \operatorname{grad}(f) + \operatorname{grad}(g)$.
- Ist o.E. f normiert, also $a_m = 1$, so hat fg den Koeffizienten b_n bei x^{m+n}, woraus sofort $\operatorname{grad}(fg) = m + n = \operatorname{grad}(f) + \operatorname{grad}(g)$ folgt.
- Ist R Integritätsring, so folgt aus $a_m \neq 0$ und $b_n \neq 0$ natürlich $a_m b_n \neq 0$, und damit $\operatorname{grad}(fg) = \operatorname{grad}(f) + \operatorname{grad}(g)$. Damit ist auch (3) bewiesen. ■

Das folgende Beispiel zeigt, dass die Formel $\operatorname{grad}(fg) = \operatorname{grad}(f) + \operatorname{grad}(g)$ nicht allgemein gilt:

Beispiel: Für $f = 1 + 2x$ in $\mathbb{Z}_4[x]$ gilt

$$f^2 = (1 + 2x)(1 + 2x) = 1,$$

also $\operatorname{grad}(fg) < \operatorname{grad}(f) + \operatorname{grad}(g)$. Außerdem gilt $1 + 2x \in (\mathbb{Z}_2[x])^*$.

Phänomene wie im letzten Beispiele passieren in Integritätsringen nicht:

SATZ. *Sei R ein Integritätsring. Dann gilt:*

(1) *Auch der Polynomring $R[x]$ ist ein Integritätsring.*
(2) *Für die Einheiten gilt: $R[x]^* = R^*$.*

Beweis: Sind $f, g \in R[x]\setminus\{0\}$, so folgt aus $\operatorname{grad}(fg) = \operatorname{grad}(f)+\operatorname{grad}(g)$ natürlich $fg \neq 0$. Sind $f, g \in R[x]$ mit $fg = 1$, so folgt

$$\operatorname{grad}(f) + \operatorname{grad}(g) = \operatorname{grad}(fg) = \operatorname{grad}(1) = 0, \quad \text{also} \quad \operatorname{grad}(f) = \operatorname{grad}(g) = 0.$$

Damit gilt $f, g \in R$, also wegen $fg = 1$ dann $f, g \in R^*$. ■

Beispiel: Da $\mathbb{Z}$ und $\mathbb{R}$ Integritätsringe sind, sind dies auch $\mathbb{Z}[x]$ und $\mathbb{R}[x]$ und es gilt

$$\mathbb{Z}[x]^* = \mathbb{Z}^* = \{\pm 1\} \quad \text{und} \quad \mathbb{R}[x]^* = \mathbb{R}^* = \mathbb{R}\setminus\{0\}.$$

Ein wichtiges Hilfsmittel im Umgang mit Polynomen ist die **Polynomdivision**: Ist R ein kommutativer Ring, sind $a, b \in R[x]$ Polynome, wobei b normiert ist, also höchsten Koeffizienten 1 hat, so liefert die Polynomdivision einen Quotienten q und einen Rest r, sodass man schreiben kann

$$a = qb + r \quad \text{mit} \quad \operatorname{grad}(r) < \operatorname{grad}(b).$$

Wir beginnen mit Beispielen:

Beispiele:

(1) Im Polynomring $\mathbb{Q}[x]$ dividieren wir $2x^4 + x^3 + 7x^2 - x + 3$ durch $x^2 + 2x + 3$:

$$\begin{array}{rcl} (2x^4 + x^3 + 7x^2 - x + 3) & : & (x^2 + 2x + 3) \quad = \quad 2x^2 - 3x + 7 \text{ Rest } -6x - 18 \\ \underline{-(2x^4 + 4x^3 + 6x^2)} & & \\ -3x^3 + x^2 - x + 3 & & \\ \underline{-(-3x^3 - 6x^2 - 9x)} & & \\ 7x^2 + 8x + 3 & & \\ \underline{-(7x^2 + 14x + 21)} & & \\ -6x - 18 & & \end{array}$$

(2) Im Polynomring $\mathbb{Z}_6[x]$ dividieren wir $2x^4 + x^3 + x^2 + 5x + 3$ durch $x^2 + 2x + 3$:

$$\begin{array}{rcl} (2x^4 + x^3 + x^2 + 5x + 3) & : & (x^2 + 2x + 3) \quad = \quad 2x^2 + 3x + 1 \text{ Rest } 0 \\ \underline{-(2x^4 + 4x^3)} & & \\ 3x^3 + x^2 + 5x + 3 & & \\ \underline{-(3x^3 \qquad + 3x)} & & \\ x^2 + 2x + 3 & & \\ \underline{-(x^2 + 2x + 3)} & & \\ 0 & & \end{array}$$

Hier ist eine algorithmische Darstellung der Polynomdivision:

Eingabe: $a, b \in R[x]$, wobei R ein kommutativer Ring und b ein normiertes Polynom ist.
Ausgabe: $q, r \in R[x]$ mit $a = qb + r$ und $\operatorname{grad}(r) < \operatorname{grad}(b)$

1: $q \leftarrow 0$
2: $r \leftarrow a$
3: **while** $\operatorname{grad}(r) \geq \operatorname{grad}(b)$ **do**
4: Sei c der höchste Koeffizient von r
5: $q \leftarrow q + cx^{\operatorname{grad}(r)-\operatorname{grad}(b)}$
6: $r \leftarrow r - cx^{\operatorname{grad}(r)-\operatorname{grad}(b)} \cdot b$
7: **end while**
8: **return** q, r

Bemerkung: In jedem Schritt des Algorithmus bleibt die Beziehung $a = qb+r$ erhalten. Dies ist trivial zu Beginn wegen $q = 0$ und $r = a$. Gilt nun $a = qb+r$ und ist $\operatorname{grad}(r) \geq \operatorname{grad}(b)$ und ist c der Leitkoeffizient von r, also $r = cx^{\operatorname{grad}(r)} + \ldots$, so können wir zerlegen

$$a = (q + cx^{\operatorname{grad}(r)-\operatorname{grad}(b)})b + (r - cx^{\operatorname{grad}(r)-\operatorname{grad}(b)}b).$$

Also bleibt die Beziehung $a = qb + r$ erhalten. Wegen

$$\text{grad}(r - cx^{\text{grad}(r)-\text{grad}(b)}b) < \text{grad}(r)$$

wird der Grad von r kleiner.

Bemerkungen:

(1) In SAGE kann man mit `R=ZZ` einen Ring vereinbaren, mit `Rx.<x>=R[]` dann einen zugehörigen Polynomring. Mit `a.quo_rem(b)` erhält man dann das Ergebnis (q, r) der Polynomdivision von a durch b.

(2) Man kann obigen Algorithmus auch direkt in SAGE schreiben:

```
def poldiv(a,b):
  if b.leading_coefficient()!=1:
    return False
  q,r=P(0),P(a)
  while r.degree()>=b.degree():
    c=r.leading_coefficient()
    q=q+c*x^(r.degree()-b.degree())
    r=r-c*x^(r.degree()-b.degree())*b
  return (q,r)
```

Satz. *Ist R ein kommutativer Ring, $R[x]$ der Polynomring in einer Unbestimmten x über R, $a, b \in R[x]$, wobei b normiert ist, so gibt es eindeutig bestimmte Polynome $q, r \in R[x]$ mit*

$$a = qb + r \quad \textit{und} \quad \text{grad}(r) < \text{grad}(b).$$

(q und r lassen sich durch Polynomdivision finden.)

Beweis:

- *Existenz*: Die Polynomdivision liefert $q, r \in R[x]$ mit $a = qb + r$ und $\text{grad}(r) < \text{grad}(b)$.
- *Eindeutigkeit:* Seien $q, r, \widetilde{q}, \widetilde{r} \in R[x]$ mit

  $$a = qb + r, \quad a = \widetilde{q}b + \widetilde{r}, \quad \text{grad}(r) < \text{grad}(b), \quad \text{grad}(\widetilde{r}) < \text{grad}(b).$$

  Dann ist

  $$0 = a - a = (\widetilde{q} - q)b + (\widetilde{r} - r), \quad \text{also} \quad r - \widetilde{r} = (\widetilde{q} - q)b.$$

  Da b normiert ist, erhalten wir mit der Gradformel

  $$\text{grad}(r - \widetilde{r}) = \text{grad}(\widetilde{q} - q) + \text{grad}(b).$$

  Wegen $\text{grad}(r - \widetilde{r}) < \text{grad}(b)$ bleibt nur die Möglichkeit

  $$\text{grad}(r - \widetilde{r}) = -\infty \quad \text{und} \quad \text{grad}(\widetilde{q} - q) = -\infty,$$

  also $\widetilde{q} = q$ und $\widetilde{r} = r$, was die Eindeutigkeit der Darstellung beweist. ■

Satz. *Ist K ein Körper und $f \in K[x]$ ein Polynom vom Grad $n \geq 1$, so hat f höchstens n Nullstellen in K, d.h.*

$$|\{a \in K : f(a) = 0\}| \leq n.$$

Beweis: Wir beweisen dies durch Induktion nach dem Grad n.

- Im Fall $\text{grad}(f) = 1$ ist $f = ax + b$ mit $a \neq 0$. Es gibt genau eine Nullstelle, nämlich $-\frac{b}{a}$.

- Sei nun $n \geq 2$ und die Aussage bereits für Polynome vom Grad $\neq n-1$ gezeigt. Hat f keine Nullstelle, so ist die Aussage richtig, wir sind fertig. Sei nun $a \in K$ mit $f(a) = 0$. Dividieren wir f durch $x - a$, so erhalten wir eine Zerlegung

$$f(x) = g(x)(x-a) + r(x) \text{ mit } g(x), r(x) \in K[x], \text{grad}(r(x)) < 1.$$

Dann ist $r(x) = r$ konstant: $f(x) = g(x)(x-a) + r$. Setzen wir nun $x = a$ ein, so ergibt sich

$$0 = f(a) = g(a)(a-a) + r, \quad \text{also} \quad r = 0,$$

und damit

$$f(x) = (x-a) \cdot g(x).$$

Natürlich gilt $\text{grad}(g) = \text{grad}(f) - 1 = n - 1$. Ist a' eine von a verschiedene Nullstelle von $f(x)$, so folgt durch Einsetzen $x = a'$

$$0 = f(a') = (a'-a)g(a'),$$

also $g(a') = 0$, d.h. a' ist eine Nullstelle von $g(x)$. Da nach Induktionsvoraussetzung g höchstens $n-1$ Nullstellen besitzt, kann f höchstens n Nullstellen haben. Dies wollten wir zeigen. ■

Wenn man statt einem Körper einen beliebigen kommutativen Ring nimmt, muss die Aussage des vorangegangenen Satzes nicht mehr stimmen, wie das folgende Beispiel zeigt:

Beispiel: Man überprüft leicht, dass das Polynom $f = x^2 + x \in \mathbb{Z}_6[x]$ die vier Nullstellen $0, 2, 3, 5$ in $\mathbb{Z}_6$ hat, obwohl das Polynom nur Grad 2 hat.

Wir folgern aus dem letzten Ergebnis folgenden wichtigen Satz:

SATZ. *Jede endliche Untergruppe G der multiplikativen Gruppe K^* eines Körpers K ist zyklisch.*

Beweis: Sei d ein Teiler der Gruppenordnung $|G|$. Wir betrachten

$$U_d = \{x \in G : x^d = 1\} \subseteq \{x \in K : x^d = 1\} = \{x \in K : x^d - 1 = 0\}.$$

Da $x^d - 1$ höchstens d Nullstellen in K besitzt, folgt

$$|U_d| \leq d.$$

Nach einem Satz über zyklische Gruppe ist dann G zyklisch. ■

FOLGERUNG. *Ist p eine Primzahl, so ist die multiplikative Gruppe $\mathbb{Z}_p^*$ des Körpers $\mathbb{Z}_p$ zyklisch. (Ein erzeugendes Element der Gruppe wird auch* **Primitivwurzel modulo** *p genannt.)*

Beispiel: Wir betrachten $\mathbb{Z}_7^*$. Es gilt (in $\mathbb{Z}_7$)

$$2^1 = 2, \quad 2^2 = 4, \quad 2^3 = 1,$$

also hat 2 die Ordnung 3 und ist kein Erzeuger von $\mathbb{Z}_7^*$.

$$3^1 = 3, \quad 3^2 = 2, \quad 3^3 = 6, \quad 3^4 = 4, \quad 3^5 = 5, \quad 3^6 = 1.$$

Also erzeugt 3 die Gruppe $\mathbb{Z}_7^*$. (Daher ist 3 eine Primitivwurzel modulo 7.)

4. Ideale

DEFINITION. *Sei R ein Ring. Ein* **Ideal** *ist eine Teilmenge $\mathfrak{a} \subseteq R$, sodass $\mathfrak{a}$ eine Untergruppe der additiven Gruppe von R ist, und sodass $R\mathfrak{a} \subseteq \mathfrak{a}$ und $\mathfrak{a}R \subseteq \mathfrak{a}$ gilt (mit $R\mathfrak{a} = \{ra : r \in R, a \in \mathfrak{a}\}$ und $\mathfrak{a}R = \{ar : a \in \mathfrak{a}, r \in R\}$). Wegen $-1 \in R$ kann man die Bedingungen auch so formulieren:*

- $0 \in \mathfrak{a}$,
- $a_1, a_2 \in \mathfrak{a} \Longrightarrow a_1 + a_2 \in \mathfrak{a}$,
- $r \in R, a \in \mathfrak{a} \Longrightarrow ra \in \mathfrak{a}$ *und* $ar \in \mathfrak{a}$. *(Ist R kommutativ, so muss man natürlich nur $ra \in \mathfrak{a}$ überprüfen.)*

Bemerkung: Ist R nicht kommutativ, so unterscheidet man zwischen **Linksidealen**, **Rechtsidealen** und **zweiseitigen Idealen**, wobei die zweiseitigen Ideale auch einfach Ideale genannt werden - wie in obiger Definition. Die Teilmenge $\mathfrak{a}$ muss bezüglich Addition eine abelsche Gruppe sein, im Fall eines linksseitigen Ideals muss $R\mathfrak{a} \subseteq \mathfrak{a}$, im Fall eines rechtsseitigen Ideals muss $\mathfrak{a}R \subseteq \mathfrak{a}$, im Fall eines zweiseitigen Ideals muss $R\mathfrak{a} \subseteq \mathfrak{a}$ und $\mathfrak{a}R \subseteq \mathfrak{a}$ gelten.

Beispiel: Wir betrachten in $\mathbb{Z}$

$$\mathbb{Z} \cdot 3 = \{3n : n \in \mathbb{Z}\} = \{0, \pm 3, \pm 6, \pm 9, \pm 12, \pm 15, \dots\}.$$

Wir überprüfen obige Bedingungen für ein Ideal:

- $0 \in \mathbb{Z} \cdot 3$ ist klar.
- Sind $3n_1, 3n_2 \in \mathbb{Z} \cdot 3$, so auch $3n_1 + 3n_2 = 3(n_1 + n_2)$.
- Ist $m \in \mathbb{Z}$ und $3n \in \mathbb{Z} \cdot 3$, so ist auch $m \cdot 3n = 3(mn) \in \mathbb{Z} \cdot 3$.

Also ist $\mathbb{Z} \cdot 3$ ein Ideal.

Beispiele:

(1) In jedem Ring R sind $\{0\}$ und R Ideale.
(2) In $\mathbb{Z}$ kennen wir die Untergruppen bzgl. der Addition, sie sind auch Ideale:
$$\mathbb{Z}\, n = \{kn : k \in \mathbb{Z}\} \text{ für } n \in \mathbb{N}_0.$$
(3) Ist K ein Körper oder Schiefkörper, so besitzt K nur die Ideale $\{0\}$ und K.
(4) Ist K ein Körper und
$$R = \mathrm{M}_2(K)$$
der Ring der 2×2-Matrizen über K, so besitzt R nur die Ideale $\{0\}$ und R.

Im Folgenden interessieren wir uns in erster Linie für Ideale in kommutativen Ringen.

DEFINITION. *Seien $\mathfrak{a}, \mathfrak{b}$ Ideale eines kommutativen Rings R.*

(1) *Die* **Summe** $\mathfrak{a} + \mathfrak{b}$ *wird durch*
$$\mathfrak{a} + \mathfrak{b} = \{a + b : a \in \mathfrak{a}, b \in \mathfrak{b}\}$$
definiert.
(2) *Der* **Durchschnitt** $\mathfrak{a} \cap \mathfrak{b}$ *ist der mengentheoretische Durchschnitt*
$$\mathfrak{a} \cap \mathfrak{b} = \{x : x \in \mathfrak{a} \text{ und } x \in \mathfrak{b}\}.$$
(3) *Das* **Produkt** $\mathfrak{a}\mathfrak{b}$ *wird definiert als*
$$\mathfrak{a}\mathfrak{b} = \{a_1 b_1 + \cdots + a_n b_n \in R : n \in \mathbb{N}, a_1, \dots, a_n \in \mathfrak{a}, b_1, \dots, b_n \in \mathfrak{b}\}.$$

LEMMA. *Seien $\mathfrak{a}, \mathfrak{b}$ Ideale eines kommutativen Rings R. Dann gilt:*

(1) *Die Summe $\mathfrak{a} + \mathfrak{b}$, der Durchschnitt $\mathfrak{a} \cap \mathfrak{b}$ und das Produkt $\mathfrak{a}\mathfrak{b}$ sind Ideale in R.*
(2) *Die Summe $\mathfrak{a} + \mathfrak{b}$ ist das kleinste Ideal, das $\mathfrak{a} \cup \mathfrak{b}$ enthält.*
(3) *$\mathfrak{a}\mathfrak{b}$ ist das kleinste Ideal, das alle Produkte ab mit $a \in \mathfrak{a}$ und $b \in \mathfrak{b}$ enthält.*

Beweis: Man überprüft, dass $\mathfrak{a}+\mathfrak{b}$, $\mathfrak{a}\cap\mathfrak{b}$ und $\mathfrak{ab}$ Ideale sind, der Rest ist dann klar. ■

Beispiele: In $\mathbb{Z}$ betrachten wir die Ideale $\mathbb{Z}\,a$ und $\mathbb{Z}\,b$ mit $a,b\in\mathbb{N}_0$. Dann gilt

$$\mathbb{Z}\,a+\mathbb{Z}\,b=\mathbb{Z}\,\mathrm{ggT}(a,b),\quad \mathbb{Z}\,a\cap\mathbb{Z}\,b=\mathbb{Z}\,\mathrm{kgV}(a,b),\quad \mathbb{Z}\,a\cdot\mathbb{Z}\,b=\mathbb{Z}\,ab.$$

Bemerkungen: Statt mit zwei Idealen kann man auch die Summe, den Durchschnitt, das Produkt von endlich vielen Idealen bilden.

DEFINITION. *Sei R ein kommutativer Ring. Sind $a_1,\dots,a_n\in R$, so definiert man $(a_1,\dots,a_n)$ durch*

$$(a_1,\dots,a_n)=Ra_1+\cdots+Ra_n=\{r_1a_1+\cdots+r_na_n : r_1,\dots,r_n\in R\}.$$

Bemerkungen:

(1) Mit der letzten Notation gilt in $\mathbb{Z}$ für $a,b\in\mathbb{Z}$

$$(a)+(b)=(a,b)=(\mathrm{ggT}(a,b)),\quad (a)\cap(b)=(\mathrm{kgV}(a,b)),\quad (a)(b)=(ab).$$

(2) In einem kommutativen Ring R gilt dann

$$(a_1,\dots,a_m)+(b_1,\dots,b_n)=(a_1,\dots,a_m,b_1,\dots,b_n)$$

und

$$(a_1\dots,a_m)(b_1,\dots,b_n)=(a_1b_1,\dots,a_1b_n,a_2b_1,\dots,a_2b_n,\dots,a_mb_1,\dots,a_mb_n).$$

(3) Folgende Bemerkung ist eigentlich trivial, aber für manche Rechnungen mit Idealen hilfreich:

$$\text{Ist } a_n\in(a_1,\dots,a_{n-1}),\ \text{so gilt } (a_1,\dots,a_n)=(a_1,\dots,a_{n-1}).$$

DEFINITION. *Sei R ein kommutativer Ring.*

(1) *Ein Ideal $\mathfrak{a}$ heißt* **endlich erzeugt***, wenn es Elemente $a_1,\dots,a_n\in R$ gibt mit*

$$\mathfrak{a}=(a_1,\dots,a_n).$$

(2) *Ein Ideal $\mathfrak{a}$ heißt ein* **Hauptideal***, wenn es ein $a\in R$ gibt mit*

$$\mathfrak{a}=(a).$$

Beispiele:

(1) In $\mathbb{Z}$ ist jedes Ideal ein Hauptideal.

(2) Wir betrachten den Polynomring $\mathbb{Z}[x]$. In diesem Ring gilt

$$\begin{aligned}(2) &= \{\sum_{i\geq 0}2a_ix^i : a_i\in\mathbb{Z}\},\\ (x) &= \{\sum_{i\geq 1}a_ix^i : a_i\in\mathbb{Z}\},\\ (2,x) &= \{2a_0+\sum_{i\geq 1}a_ix^i : a_i\in\mathbb{Z}\}.\end{aligned}$$

Wir betrachten das Ideal $\mathfrak{a}=(2,x)$. Angenommen, $\mathfrak{a}$ wäre ein Hauptideal (a). Dann gäbe es Polynome b,c mit $2=ab$ und $x=ac$. Mit der Gradformel folgt $\mathrm{grad}(a)=\mathrm{grad}(b)=0$, also $a,b\in\mathbb{Z}$, und damit $a\in\{\pm1,\pm2\}$. Wegen $1\notin(2,x)$ ist $a\neq\pm1$. Wegen $x\notin(2)$ ist $a\neq\pm2$. Also ist die Annahme falsch, d.h. $(2,x)$ kein Hauptideal.

Da wir in Erlangen sind, erwähnen wir folgende Definition zur Erinnerung an Emmy Noether:

DEFINITION. *Ein kommutativer Ring R heißt* **noetherscher Ring***, wenn jedes Ideal von R endlich erzeugt ist.*

Bemerkung: Ein Beispiel eines nichtnoetherschen Ringes ist folgender Unterring des Polynomrings $\mathbb{Q}[x]$:

$$R=\{f\in\mathbb{Q}[x] : f(n)\in\mathbb{Z}\text{ für alle }n\in\mathbb{Z}\}.$$

5. Ringhomomorphismen

DEFINITION. *Ein* **Ringhomomorphismus** *zwischen zwei Ringen R und S ist eine Abbildung $\phi : R \to S$, sodass für alle $x, y \in R$ gilt*

$$\phi(x+y) = \phi(x) + \phi(y), \quad \phi(xy) = \phi(x)\phi(y), \quad \phi(1) = 1.$$

Der **Kern** *von ϕ ist*

$$\mathrm{Kern}(\phi) = \phi^{-1}(0) = \{x \in R : \phi(x) = 0\}.$$

Ein **Ringisomorphismus** *ist ein bijektiver Ringhomomorphismus. (Dann ist auch die Umkehrabbildung ein Ringhomomorphismus.)*

Bemerkung: Da ein Ringhomomorphismus $\phi : R \to S$ auch ein Homomorphismus der additiven Gruppen $(R, +)$ und $(S, +)$ ist, gilt natürlich

$$\phi(0) = 0 \quad \text{und} \quad \phi(-x) = -\phi(x).$$

Bemerkung: Folgende Schreibweise für abelsche Gruppen benutzen wir auch für die additive Gruppe eines Rings R: Für $n \in \mathbb{Z}$ und $x \in R$ ist $n \cdot x$ definiert durch

$$n \cdot x = \begin{cases} \sum_{i=1}^{n} x & \text{für } n \geq 1, \\ 0 & \text{für } n = 0, \\ -\sum_{i=1}^{|n|} x & \text{für } n \leq -1. \end{cases}$$

Für $m, n \in \mathbb{Z}$ und $x \in R$ gilt dann

$$(m+n) \cdot x = m \cdot x + n \cdot x \quad \text{und} \quad (mn) \cdot x = m \cdot (n \cdot x).$$

Mit dieser Schreibweise können wir einen wichtigen Ringhomomorphismus angeben:

SATZ. *Ist R ein Ring, so gibt es genau einen Ringhomomorphismus $\phi : \mathbb{Z} \to R$, der durch*

$$\phi(n) = n \cdot 1_R$$

gegeben ist, wobei 1_R die Eins in R bezeichnet.

Die Eindeutigkeit folgt direkt aus $\phi(1) = 1_R$, der Rest aus den zuvor angegebenen Formeln.

SATZ. *Ist $\phi : R \to S$ ein Ringhomomorphismus, so gilt:*

1. $\mathrm{Kern}(\phi)$ *ist ein Ideal in R.*
2. $\phi(R)$ *ist ein Unterring von S.*
3. ϕ *ist genau dann injektiv, wenn* $\mathrm{Kern}(\phi) = \{0\}$ *ist. (In diesem Fall ist $R \simeq \phi(R) \subseteq S$.)*
4. *Es ist $\phi(R^*) \subseteq S^*$ und $\phi_{R^*} : R^* \to S^*$ ist ein Gruppenhomomorphismus.*

Beweis:

1. Wir überprüfen die Eigenschaften eines Ideals:
   - $0 \in \mathrm{Kern}(\phi)$ folgt aus $\phi(0) = 0$.
   - Sind $a, b \in \mathrm{Kern}(\phi)$, also $\phi(a) = \phi(b) = 0$, so gilt $\phi(a+b) = \phi(a) + \phi(b) = 0 + 0 = 0$, also $a + b \in \mathrm{Kern}(\phi)$.
   - Sei nun $a \in \mathrm{Kern}(\phi)$, also $\phi(a) = 0$, und $r \in R$. Dann gilt
     $$\phi(ra) = \phi(r)\phi(a) = \phi(r) \cdot 0 = 0 \quad \text{und} \quad \phi(ar) = \phi(a)\phi(r) = 0 \cdot \phi(r) = 0,$$
     also $ra \in \mathrm{Kern}(\phi)$ und $ar \in \mathrm{Kern}(\phi)$.

   Also ist $\mathrm{Kern}(\phi)$ ein Ideal in R.
2. Dies folgt aus
   $$\phi(0) = 0, \quad \phi(x) + \phi(y) = \phi(x+y), \quad 1 = \phi(1), \quad \phi(x)\phi(y) = \phi(xy).$$
3. Da ϕ ein Gruppenhomomorphismus zwischen den abelschen Gruppen $(R, +)$ und $(S, +)$ ist, folgt die Aussage aus der entsprechenden Aussage für Gruppen.

(4) Ist $r \in R^*$, so gibt es ein $r' \in R$ mit $rr' = r'r = 1$. Dann gilt aber $\phi(r)\phi(r') = \phi(rr') = \phi(1) = 1$ und $\phi(r')\phi(r) = \phi(r'r) = \phi(1) = 1$, also ist $\phi(r) \in S^*$. Der Rest ist klar. ■

SATZ. *Ist K ein Körper und $\phi : K \to R$ ein Ringhomomorphismusm, so ist $R = \{0\}$ oder ϕ ist injektiv.*

Beweis: Kern(ϕ) ist ein Ideal in K, also $\{0\}$ oder K. Ist Kern(ϕ) $= \{0\}$, so ist ϕ injektiv. Ist Kern(ϕ) $= K$, so gilt $1 = \phi(1) = \phi(0) = 0$, also ist R der Nullring. ■

Der folgende Satz beschreibt nochmals, dass man in Polynome einsetzen darf.

SATZ (Einsetzungshomomorphismus). *Sei R ein kommutativer Ring, S ein kommutativer Oberring von R und $\alpha \in S$. Dann gibt es genau einen Ringhomomorphismus $\phi : R[x] \to S$ mit $\phi(r) = r$ für $r \in R$ und $\phi(x) = \alpha$. Er ist gegeben durch*

$$\phi(\sum_{i\geq 0} a_i x^i) = \sum_{i\geq 0} a_i \alpha^i, \qquad \textit{oder anders geschrieben} \qquad \phi(f(x)) = f(\alpha).$$

Beweis: Ist $\phi : R[x] \to S$ ein Ringhomomorphismus mit $\phi(r) = r$ für alle $r \in R$ und $\phi(x) = \alpha$, so gilt

$$\phi(\sum_{i\geq 0} a_i x^i) = \sum_{i\geq 0} \phi(a_i)\phi(x)^i = \sum_{i\geq 0} a_i \alpha^i.$$

Daher ist ϕ durch die Vorgaben eindeutig bestimmt. Die Rechenregeln für Polynome zeigen, dass ϕ ein Ringhomomorphismus ist. ■

Beispiel: $\mathbb{Z}$ ist ein Unterring von $\mathbb{C}$. Daher wird durch

$$\phi : \mathbb{Z}[x] \to \mathbb{C} \text{ mit } \phi(x) = \phi(i)$$

ein Ringhomomorphismus definiert. Das Bild ist

$$\phi(\mathbb{Z}[x]) = \mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}.$$

Was ist der Kern von ϕ? Es ist $i^2 = -1$, also $i^2 + 1 = 0$. Daher ist $x^2 + 1 \in$ Kern(ϕ).
Behauptung: Kern(ϕ) $= (x^2 + 1)$.
Beweis: $\supseteq$ Ist $f(x) \in (x^2 + 1)$, so gibt es ein Polynom $g(x) \in \mathbb{Z}[x]$ mit $f(x) = g(x)(x^2 + 1$. Dann ist $\phi(f(x)) = f(i) = g(i)(i^2 + 1) = 0$, also $f(x) \in$ Kern(ϕ).
Sei nun $f(x) \in$ Kern(ϕ), d.h. $f(i) = 0$. Wir dividieren $f(x)$ durch $x^2 + 1$ und erhalten $g(x) \in \mathbb{Z}[x]$ und $a, b \in \mathbb{Z}$ mit

$$f(x) = g(x)(x^2 + 1) + ax + b.$$

Setzen wir $x = i$ ein, so ergibt sich

$$0 = f(i) = g(i)(i^2 + 1) + ai + b = ai + b,$$

woraus $a = b = 0$ folgt, da i kein rationale Zahl ist. Also ist $f(x) = g(x)(x^2 + 1)$, d.h. $f(x) \in (x^2 + 1)$, was wir zeigen wollten.

LEMMA. *Seien R und S kommutative Ringe und $\phi : R \to S$ ein Ringhomomorphismus. Dann definiert*

$$R[x] \to S[x], \quad \sum_{i\geq 0} a_i x^i \mapsto \sum_{i\geq 0} \phi(a_i) x^i$$

einen Ringhomomorphismus.

Setzt man die vorangegangenen Aussagen zusammen, so erhält man folgenden Satz:

SATZ. *Sei $\phi : R \to S$ ein Ringhomomorphismus kommutativer Ringe und $\alpha \in S$. Dann gibt es genau einen Ringhomomorphismus $\Phi : R[x] \to S$ mit $\Phi(r) = \phi(r)$ für $r \in R$ und $\Phi(x) = \alpha$, nämlich*

$$\Phi(\sum_{i\geq 0} a_i x^i) = \sum_{i\geq 0} \phi(a_i)\alpha^i.$$

Beispiel: Sei K ein Körper und $A \in \mathrm{M}_n(K)$. Dann ist

$$\phi : K \to \mathrm{M}_n(K), \quad r \mapsto r \cdot \mathbf{1}_n$$

ein injektiver Ringhomomorphismus. Wir schreiben $K[A]$ für den von $\phi(K)$ und A erzeugten Unterring von $\mathrm{M}_n(K)$:

$$K[A] = \{a_0 \cdot \mathbf{1}_n + a_1 \cdot A + a_2 \cdot A^2 + \cdots : a_0, a_1, a_2 \in K\}.$$

$K[A]$ ist ein kommutativer Unterring von $\mathrm{M}_n(K)$. Daher existiert genau ein Ringhomomorphismus

$$\Phi : K[x] \to K[A] \text{ mit } \Phi(r) = r \cdot \mathbf{1}_n \text{ für } r \in K \text{ und } \Phi(x) = A.$$

In der Linearen Algebra lernt man, dass der Kern von Φ vom Minimalpolynom von A erzeugt wird.

6. Faktorringe

Sei R ein Ring und $\mathfrak{a}$ ein Ideal in R. Bezüglich der Addition ist dann $\mathfrak{a}$ eine Untergruppe von R. Wir haben dann bereits die Faktorgruppe $R/\mathfrak{a}$ definiert. Wir wiederholen kurz die Konstruktion.

Der **Faktorring** $R/\mathfrak{a}$**:** Sei R ein (nicht notwendig kommutativer) Ring und $\mathfrak{a}$ ein Ideal in R.

(1) Durch

$$x \equiv y \bmod \mathfrak{a} \quad \Longleftrightarrow \quad x - y \in \mathfrak{a}$$

wird eine Äquivalenzrelation auf R definiert, die **Kongruenz modulo** $\mathfrak{a}$. Die Äquivalenzklasse von x bezeichnen wir mit $\overline{x}$. Als Menge ist

$$\overline{x} = x + \mathfrak{a} = \{x + a : a \in \mathfrak{a}\}.$$

Es gilt dann

$$x \equiv y \bmod \mathfrak{a} \quad \Longleftrightarrow \quad \overline{x} = \overline{y}.$$

Sei $R/\mathfrak{a}$ die Menge der Äquivalenzklassen, also

$$R/\mathfrak{a} = \{\overline{x} : x \in R\}.$$

Die kanonische Abbildung

$$\pi : R \to R/\mathfrak{a} \text{ mit } \pi(x) = \overline{x}$$

ist offensichtlich surjektiv.

(2) **Addition:** Seien $x, x', y, y' \in R$ mit

$$x \equiv x' \bmod \mathfrak{a} \quad \text{und} \quad y \equiv y' \bmod \mathfrak{a}.$$

Dann gibt es $a, b \in \mathfrak{a}$ mit

$$x' = x + a, \quad y' = y + b.$$

Es folgt $(x' + y') - (x + y) = a + b \in \mathfrak{a}$, also

$$x + y \equiv x' + y' \bmod \mathfrak{a}.$$

Anders geschrieben:

$$\overline{x} = \overline{x'} \text{ und } \overline{y} = \overline{y'} \quad \Longrightarrow \quad \overline{x + y} = \overline{x' + y'}.$$

Daher wird durch

$$\overline{x} + \overline{y} = \overline{x + y}$$

eine wohldefinierte Verknüpfung (Addition) auf $R/\mathfrak{a}$ definiert. Wir haben bereits früher gesehen, dass $(R/\mathfrak{a}, +)$ eine abelsche Gruppe ist mit neutralem Element $\overline{0}$. (Für das additive Inverse gilt $-\overline{x} = \overline{-x}$.)

(3) **Multiplikation:** Seien $x, x', y, y' \in R$ mit

$$x \equiv x' \bmod \mathfrak{a} \quad \text{und} \quad y \equiv y' \bmod \mathfrak{a}.$$

Dann gibt es $a, b \in \mathfrak{a}$ mit

$$x' = x + a, \quad y' = y + b.$$

Es folgt

$$x'y' - xy = (x+a)(y+b) - xy = (xy + xb + ay + ab) - (xy) = xb + ay + ab \in \mathfrak{a}$$

wegen $xb, ay, ab \in \mathfrak{a}$, also

$$xy \equiv x'y' \bmod \mathfrak{a}.$$

Anders geschrieben:

$$\overline{x} = \overline{x'} \text{ und } \overline{y} = \overline{y'} \quad \Longrightarrow \quad \overline{xy} = \overline{x'y'}.$$

Daher wird durch

$$\overline{x} \cdot \overline{y} = \overline{x \cdot y}$$

eine wohldefinierte Verknüpfung (Multiplikation) auf $R/\mathfrak{a}$ definiert. Wir zeigen, dass $(R/\mathfrak{a}, \cdot)$ ein Monoid ist:

- Es gilt das Assoziativgesetz:

$$\overline{x} \cdot (\overline{y} \cdot \overline{z}) = \overline{x} \cdot \overline{y \cdot z} = \overline{x \cdot (y \cdot z)} = \overline{(x \cdot y) \cdot z} = \overline{x \cdot y} \cdot \overline{z} = (\overline{x} \cdot \overline{y}) \cdot \overline{z}.$$

- $\overline{1}$ ist neutrales Element der Multiplikation:

$$\overline{1} \cdot \overline{x} = \overline{1 \cdot x} = \overline{x} = \overline{x \cdot 1} = \overline{x} \cdot \overline{1}.$$

(4) Es gelten die Distributivgesetze:

$$\overline{x} \cdot (\overline{y} + \overline{z}) = \overline{x} \cdot \overline{y+z} = \overline{x \cdot (y+z)} = \overline{x \cdot y + x \cdot z} = \overline{x \cdot y} + \overline{x \cdot z} = \overline{x} \cdot \overline{y} + \overline{x} \cdot \overline{z},$$
$$(\overline{x} + \overline{y}) \cdot \overline{z} = \overline{x+y} \cdot \overline{z} = \overline{(x+y) \cdot z} = \overline{x \cdot z + y \cdot z} = \overline{x \cdot z} + \overline{y \cdot z} = \overline{x} \cdot \overline{z} + \overline{y} \cdot \overline{z}.$$

(5) Daher ist $(R/\mathfrak{a}, +, \cdot)$ ein Ring, der **Faktorring** von R nach $\mathfrak{a}$ oder von R modulo $\mathfrak{a}$. Die Abbildung $\pi : R \to R/\mathfrak{a}$ mit $\pi(x) = \overline{x}$ wird auch als kanonische Abbildung bezeichnet und ist ein surjektiver Ringhomomorphismus mit Kern $\mathfrak{a}$.

Bemerkunge: Im Fall $\mathfrak{a} = \{0\}$ gilt:

$$\overline{x} = \overline{y} \quad \Longleftrightarrow \quad x \equiv y \bmod \mathfrak{a} \quad \Longleftrightarrow \quad x - y \in \{0\} \quad \Longleftrightarrow \quad x = y,$$

Wir können also $R/\{0\}$ mit R identifizieren.
Im Fall $\mathfrak{a} = R$ gilt für $x \in R$:

$$x \in R \quad \Longrightarrow \quad x \in \mathfrak{a} \quad \Longrightarrow \quad x \equiv 0 \bmod \mathfrak{a} \quad \Longrightarrow \quad \overline{x} = \overline{0}.$$

R/R besteht also nur aus einem Element, ist daher der Nullring.

Beispiel: Wir betrachten in $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ das Ideal $\mathfrak{a} = (1+i)$. Wegen $(1-i)(1+i) = 2$ ist $2 \in \mathfrak{a}$. Daher haben wir

$$2 \equiv 0 \bmod \mathfrak{a} \quad \text{und} \quad i \equiv -1 \equiv 1 \bmod \mathfrak{a}.$$

Es ist also

$$a + bi \equiv a + b \equiv ((a+b) \bmod 2) \bmod \mathfrak{a}.$$

Es gibt also höchstens die Restklassen $\overline{0}$ und $\overline{1}$ modulo $\mathfrak{a}$. Es gilt

$$\begin{aligned}
\overline{1} = \overline{0} \quad &\Longleftrightarrow \quad 1 \equiv 0 \bmod \mathfrak{a} \quad \Longleftrightarrow \quad 1 \in \mathfrak{a} \quad \Longleftrightarrow \\
&\Longleftrightarrow \quad 1 = (a+bi)(1+i) \text{ mit Zahlen } a, b \in \mathbb{Z} \quad \Longrightarrow \\
&\Longrightarrow \quad 1 = |a+bi|^2 \cdot |1+i|^2 \text{ mit Zahlen } a, b \in \mathbb{Z} \quad \Longrightarrow \\
&\Longrightarrow \quad 1 = (a^2 + b^2) \cdot 2 \text{ mit Zahlen } a, b \in \mathbb{Z}.
\end{aligned}$$

Die rechte Seite ist aber falsch, da 1 kein Vielfaches von 2 in $\mathbb{Z}$ ist. Also gilt

$$\overline{1} \neq \overline{0}, \quad \text{und damit} \quad \mathbb{Z}[i]/(1+i) = \{\overline{0}, \overline{1}\}.$$

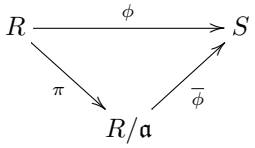
SATZ (Faktorisierungssatz). *Sei $\phi : R \to S$ ein Ringhomomorphismus und $\mathfrak{a} \subseteq R$ ein Ideal mit $\mathfrak{a} \subseteq \mathrm{Kern}(\phi)$. Dann gibt es genau einen Ringhomomorphismus*

$$\overline{\phi} : R/\mathfrak{a} \to S,$$

sodass gilt

$$\phi = \overline{\phi} \circ \pi.$$

ϕ „faktorisiert“ also über $R/\mathfrak{a}$. Dies drückt sich auch in folgendem sogenannten kommutativen Diagramm aus:



Weiter gilt:

- *Ist $\mathfrak{a} = \mathrm{Kern}(\phi)$, so ist $\overline{\phi} : R/\mathrm{Kern}(\phi) \to S$ injektiv.*
- *Ist $\mathfrak{a} = \mathrm{Kern}(\phi)$ und ϕ surjektiv, so ist $\overline{\phi}$ ein Isomorphismus:*

$$R/\mathrm{Kern}(\phi) \xrightarrow{\simeq} S.$$

Beweis:

- *Eindeutigkeit:* Ist $\overline{\phi}$ mit $\phi = \overline{\phi} \circ \pi$, so gilt für $x \in R$

  $$\phi(x) = (\overline{\phi} \circ \pi)(x) = \overline{\phi}(\pi(x)) = \overline{\phi}(\overline{x}).$$

  $\overline{\phi}$ ist also durch ϕ eindeutig bestimmt.
- *Existenz:* Seien $x, x' \in R$ mit $\overline{x} = \overline{x'}$. Dann gilt $x \equiv x' \bmod \mathfrak{a}$, d.h. es gibt ein $a \in \mathfrak{a}$ mit $x' = x + a$. Nach Voraussetzung ist $\mathfrak{a} \subseteq \mathrm{Kern}(\phi)$, also $\phi(a)0$, und damit $\phi(x') = \phi(x)$. Daher ist $\overline{\phi} : R/\mathfrak{a} \to R$ durch

  $$\overline{\phi}(\overline{x}) = \phi(x)$$

  wohldefiniert. Dass $\overline{\phi}$ ein Ringhomomorphismus ist, rechnet man nun einfach nach.
- *Fall* $\mathrm{Kern}(\phi) = \mathfrak{a}$*:* Sei $\overline{\phi}(\overline{x}) = \overline{\phi}(\overline{y})$. Dann ist $\phi(x) = \phi(y)$, also $\phi(y - x) = 0$ und damit $y - x \in \mathrm{Kern}(\phi) = \mathfrak{a}$, also $x \equiv y \bmod \mathfrak{a}$ und damit $\overline{x} = \overline{y}$. Dies beweist die Injektivität von $\overline{\phi}$.
- Der Rest ist dann klar. ■

Beispiele:

(1) Ist $n \in \mathbb{N}$, so wird durch

$$\mathbb{Z} \to \mathbb{Z}_n, \quad a \mapsto (a \bmod n)$$

ein surjektiver Ringhomomorphismus definiert mit Kern $\mathbb{Z}\, n = (n)$. Daher gilt

$$\mathbb{Z}/(n) \simeq \mathbb{Z}_n.$$

Statt $\mathbb{Z}_n$ findet man auch oft die Schreibweise $\mathbb{Z}/(n)$ oder $\mathbb{Z}/n\mathbb{Z}$ oder $\mathbb{Z}/\mathbb{Z}n$.

(2) Wir haben gesehen, dass

$$\phi : \mathbb{Z}[x] \to \mathbb{Z}[i] \text{ mit } \phi(x) = i$$

ein surjektiver Ringhomomorphismus ist mit $\mathrm{Kern}(\phi) = (x^2 + 1)$. Also erhalten wir einen Isomorphismus

$$\mathbb{Z}[x]/(x^2 + 1) \simeq \mathbb{Z}[i].$$

Der folgende Satz verallgemeinert das letzte Beispiel:

SATZ. *Sei $d \in \mathbb{Z}$ keine Quadratzahl, d.h. $d \in \mathbb{Z} \setminus \{n^2 : n \in \mathbb{N}_0\}$. Sei $\sqrt{d}$ eine Quadratwurzel aus d in $\mathbb{C}$. Dann gilt*

$$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbb{Z}\}$$

und für $a, b, a', b' \in \mathbb{Z}$

$$a + b\sqrt{d} = a' + b'\sqrt{d} \quad \Longleftrightarrow \quad a = a' \text{ und } b = b'.$$

Der eindeutig bestimmte Ringhomomorphismus $\phi : \mathbb{Z}[x] \to \mathbb{Z}[\sqrt{d}]$ mit $\phi(x) = \sqrt{d}$ induziert einen Ringisomorphismus

$$\mathbb{Z}[x]/(x^2 - d) \simeq \mathbb{Z}[\sqrt{d}].$$

Beweis:

- Aus
$$(a_1 + b_1\sqrt{d}) + (a_2 + b_2\sqrt{d}) = (a_1 + a_2) + (b_1 + b_2)\sqrt{d}$$
und
$$(a_1 + b_1\sqrt{d})(a_2 + b_2\sqrt{d}) = (a_1a_2 + db_1b_2) + (a_1b_2 + a_2b_1)\sqrt{d}$$
folgt zusammen mit
$$0, 1 \in \{a + b\sqrt{d} : a, b \in \mathbb{Z}\} \quad \text{und} \quad -(a + b\sqrt{d}) = (-a) + (-b)\sqrt{d},$$
dass $\{a + b\sqrt{d} : a, b \in \mathbb{Z}\}$ der kleinste $\mathbb{Z}$ und $\sqrt{d}$ enthaltende Unterring von $\mathbb{C}$ ist, d.h.
$$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbb{Z}\}.$$
- Es gilt für $a, b, a', b' \in \mathbb{Z}$
$$a + b\sqrt{d} = a' + b'\sqrt{d} \quad \Longleftrightarrow \quad a - a' = (b' - b)\sqrt{d}.$$
Wäre $b \neq b'$, so wäre $d = (\frac{a-a'}{b'-b})^2$, also d ein Quadrat in $\mathbb{Q}$, und damit auch in $\mathbb{Z}$, was aber ausgeschlossen war. Es muss also $b = b'$ gelten, und damit natürlich auch $a = a'$.
- Wir zeigen zunächst, dass
$$\text{Kern}(\phi) = (x^2 - d)$$
gilt.
Wegen $\phi(x^2 - d) = \phi(x)^2 - d = (\sqrt{d})^2 - d = 0$, ist die Inklusion $\supseteq$ klar.
Sei umgekehrt $f(x) \in \text{Kern}(\phi)$. Wir dividieren $f(x)$ durch $x^2 - d$ und erhalten eine Darstellung
$$f(x) = g(x)(x^2 - d) + (a + bx) \quad \text{mit} \quad g(x) \in \mathbb{Z}[x], \quad a, b \in \mathbb{Z}.$$
Setzen wir $x = \sqrt{d}$ ein, so ergibt sich
$$0 = a + b\sqrt{d}.$$
Daraus folgt aber $a = b = 0$, und damit $f(x) = g(x)(x^2 - d) \in (x^2 - d)$.
Damit ist die Behauptung bewiesen.
- Der Faktorisierungssatz liefert nun sofort
$$\mathbb{Z}[x]/(x^2 - d) \simeq \mathbb{Z}[\sqrt{d}],$$
was noch zu zeigen war. ■

Der folgende Satz zeigt eine Möglichkeit, aus bekannten Ringen neue Ringe zu gewinnen.

SATZ. *Sei R ein kommutativer Ring und $f \in R[x]$ ein normiertes Polynom vom Grad $n \geq 1$. Dann ist*

$$\{a_0 + a_1x + \cdots + a_{n-1}x^{n-1} : a_0, a_1, \ldots, a_{n-1} \in R\}$$

ein Repräsentantensystem für den Faktorring $R[x]/(f)$, insbesondere kann man R als Unterring von $R[x]/(f)$ auffassen.
Ist ξ das Bild von x in $R[x]/(f)$, so ist

$$R[x]/(f) = \{a_0 + a_1\xi + \cdots + a_{n-1}\xi^{n-1} : a_0, a_1, \ldots, a_{n-1} \in R\}.$$

Ist $f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_1x + c_0$, so genügt ξ der Gleichung

$$\xi^n = -c_0 - c_1\xi - \cdots - c_{n-1}\xi^{n-1}.$$

Beweis: Sei $a(x) \in R[x]$ ein beliebiges Polynom. Dividieren wir durch $f = x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0$, so erhalten wir eine Darstellung

$$a(x) = b(x)f(x) + (a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}) \quad \text{mit } b(x) \in R[x] \text{ und } a_0, a_1, \ldots, a_{n-1} \in R.$$

Dann ist

$$a(x) \equiv a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \bmod (f).$$

Gilt nun

$$a_0 + a_1 x + \cdots + a_n x^{n-1} \equiv b_0 + b_1 x + \cdots + b_{n-1}x^{n-1} \bmod (f),$$

so gibt es ein Polynom $g(x) \in R[x]$ mit

$$(a_0 - b_0) + (a_1 - b_1)x + \cdots + (a_{n-1} - b_{n-1})x^{n-1} = g(x)f(x).$$

Wäre $g(x) \neq 0$, so wäre $\operatorname{grad}(g(x)f(x)) = \operatorname{grad}(g(x)) + \operatorname{grad}(f(x)) \geq \operatorname{grad}(f(x)) = n$, was offensichtlich nicht sein kann. Also ist $g(x) = 0$ und damit

$$a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} = b_0 + b_1 x + \cdots + b_{n-1}x^{n-1}.$$

Daher ist

$$\{a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} : a_0, a_1, \ldots, a_{n-1} \in R\}$$

ein Repräsentantensystem von $R[x]/(f)$. Insbesondere gilt für $a, a' \in R$

$$\overline{a} = \overline{a'} \quad \Longleftrightarrow \quad a = a'.$$

Wir können also R auch als Teilmenge von $R[x]/(f)$ auffassen und schreiben $\overline{a} = a$ für $a \in R$. Mit $\xi = \overline{x}$ gilt dann

$$\begin{aligned} R[x]/(f) &= \{\overline{a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}} : a_0, a_1, \ldots, a_{n-1} \in R\} = \\ &= \{a_0 + a_1\overline{x} + \cdots + a_{n-1}\overline{x}^{n-1} : a_0, a_1, \ldots, a_{n-1} \in R\} = \\ &= \{a_0 + a_1\xi + \cdots + a_{n-1}\xi^{n-1} : a_0, a_1, \ldots, a_{n-1} \in R\}. \end{aligned}$$

Nun gilt

$$c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} + x^n \equiv 0 \bmod (f),$$

also

$$\begin{aligned} 0 &= \overline{c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} + x^n} = c_0 + c_1\overline{x} + \cdots + c_{n-1}\overline{x}^{n-1} + \overline{x}^n = \\ &= c_0 + c_1\xi + \cdots + c_{n-1}\xi^{n-1} + \xi^n, \end{aligned}$$

woraus

$$\xi^n = -c_0 - c_1\xi - \cdots - c_{n-1}\xi^{n-1}$$

folgt. ■

Charakteristik eines Rings: Sei R ein Ring. Es gibt genau einen Ringhomomorphismus

$$\phi : \mathbb{Z} \to R,$$

der durch $\phi(1) = 1_R$ festgelegt ist. Der Kern ist ein Ideal in $\mathbb{Z}$.

- **Fall** $\operatorname{Kern}(\phi) = \{0\}$**:** Wir sagen, R **hat Charakteristik** 0. Für alle $n \in \mathbb{N}$ ist

  $$n \cdot 1_R = \sum_{i=1}^{n} 1_R \neq 0.$$

  Es ist $\phi(\mathbb{Z}) \simeq \mathbb{Z}$. Wir können $\mathbb{Z}$ als Unterring von R auffassen.
- **Fall** $\operatorname{Kern}(\phi) = \mathbb{Z}n$ **mit** $n \in \mathbb{N}$**:** Dann ist

  $$\sum_{i=1}^{k} 1_R \neq 0 \text{ für } 1 \leq k \leq n-1 \quad \text{und} \quad \sum_{i=1}^{n} 1_R = 0.$$

  Wir sagen, R **hat Charakteristik** n. Dann ist $\phi(\mathbb{Z}) \simeq \mathbb{Z}/(n) \simeq \mathbb{Z}_n$. Wir können also $\mathbb{Z}_n$ als Unterring von R auffassen.

7. Primideale und maximale Ideale

DEFINITION. *Sei R ein kommutativer Ring.*

(1) *Ein Ideal $\mathfrak{p}$ von R wird* **Primideal** *genannt, wenn $R/\mathfrak{p}$ ein Integritätsring ist.*
(2) *Ein Ideal $\mathfrak{m}$ von R wird* **maximales Ideal** *genannt, wenn $R/\mathfrak{m}$ ein Körper ist.*

Beispiele:

(1) Die Ideale in $\mathbb{Z}$ sind (n) mit $n \in \mathbb{N}_0$. Es ist
$$\mathbb{Z}/(n) \simeq \mathbb{Z}_n.$$
   (a) Die Primideale von $\mathbb{Z}$ sind (0) und (p) für Primzahlen p.
   (b) Die maximalen Ideale von $\mathbb{Z}$ sind (p) für Primzahlen p.
(2) Da jeder Körper ein Integritätsring ist, ist klar, dass jedes maximale Ideal auch ein Primideal ist.
(3) Wir haben gesehen, dass $\mathbb{Z}[i]/(1+i) \simeq \mathbb{F}_2$ gilt. Also ist $(1+i)$ ein maximales Ideal in $\mathbb{Z}[i]$.

LEMMA. *Für einen kommutativen Ring R und ein Ideal $\mathfrak{p}$ sind äquivalent:*

(1) *$\mathfrak{p}$ ist Primideal.*
(2) *$\mathfrak{p} \neq R$ und für $x, y \in R$ gilt die Implikation*
$$xy \in \mathfrak{p} \quad \Longrightarrow \quad x \in \mathfrak{p} \text{ oder } y \in \mathfrak{p}.$$

LEMMA. *Für einen kommutativen Ring R und ein Ideal $\mathfrak{m}$ sind äquivalent:*

(1) *$\mathfrak{m}$ ist maximales Ideal.*
(2) *$\mathfrak{m} \neq R$ und für jedes Ideal $\mathfrak{a}$ von R gilt die Implikation*
$$\mathfrak{m} \subseteq \mathfrak{a} \subseteq R \quad \Longrightarrow \quad \mathfrak{a} = \mathfrak{m} \text{ oder } \mathfrak{a} = R.$$

Für den Beweis des folgendes Satzes benötigen wir ein tieferliegendes Hilfsmittel, dass sogenannte **Zornsche Lemma**:

SATZ. *Ist R ein kommutativer Ring und $\mathfrak{a}$ ein von R verschiedenes Ideal in R, so gibt es ein maximales Ideal $\mathfrak{m}$ in R mit $\mathfrak{a} \subseteq \mathfrak{m}$. (Jedes von R verschiedene Ideal ist in einem maximalen Ideal enthalten.)*

Ein Beweis des Satzes findet sich im Anhang.

LEMMA. *Ist $\phi : R \to S$ ein Ringhomomorphismus und $\mathfrak{P}$ ein Primideal ist S, so ist $\mathfrak{p} = \phi^{-1}(\mathfrak{P})$ ein Primideal in R.*

Beweis: Der Kern des natürlichen Homomorphismus
$$R \to S \to S/\mathfrak{P}$$
ist offensichtlich $\mathfrak{p} = \phi^{-1}(\mathfrak{P})$, sodass wir eine Einbettung
$$R/\mathfrak{p} \hookrightarrow S/\mathfrak{P}$$
erhalten. Da $S/\mathfrak{P}$ ein Integritätsring ist, ist auch $R/\mathfrak{p}$ als Unterring eines Integritätsrings ein Integritätsring, $\mathfrak{p}$ also ein Primideal. ■

8. Der chinesische Restsatz

Wir beginnen mit einem Beispiel zur Motiviation:

Beispiel: Ein aus Großbuchstaben bestehender „Text“ wurde von Anne, Barbara und Christa abgeschrieben. Anne schrieb in jede Zeile - bis auf die letzte - genau 80 Buchstaben, in der letzten Zeile blieben 8 Buchstaben übrig. Barbara schrieb in jede Zeile - bis auf die letzte - 81 Buchstaben, die letzte Zeile enthält aber nur 31 Buchstaben. Christa schrieb in jede Zeile - bis auf die letzte - 79 Buchstaben, die letzte enthält bei ihr aber nur 66 Buchstaben. Ist z_A, z_B, z_C die Anzahl der vollständig gefüllten Zeilen bei Anne, Barbara und Christa, so gilt also, wenn x die Anzahl der Zeichen bezeichnet:

$$x = z_A \cdot 80 + 8, \quad x = z_B \cdot 81 + 31, \quad x = z_C \cdot 79 + 66.$$

Man erhält daraus folgendes Kongruenzgleichungssystem:

$$x \equiv \begin{cases} 8 \bmod 80, \\ 31 \bmod 81, \\ 66 \bmod 79. \end{cases}$$

Mit solchen Kongruenzgleichungssystemen beschäftigt sich der chinesische Restsatz.

Definition. *Zwei Ideale $\mathfrak{a}, \mathfrak{b}$ eines kommutativen Rings heißen* **teilerfremd**, *wenn $\mathfrak{a} + \mathfrak{b} = R$ gilt. Dies ist gleichwertig damit, dass es $\widetilde{a} \in \mathfrak{a}$ und $\widetilde{b} \in \mathfrak{b}$ gibt mit $\widetilde{a} + \widetilde{b} = 1$.*

Bemerkungen: Wir betrachten den Ring $\mathbb{Z}$.

(1) In $\mathbb{Z}$ gilt
$$(a) + (b) = (\mathrm{ggT}(a, b)).$$
Die Ideale (a) und (b) sind also genau dann teilerfremd, wenn a und b teilerfremd sind, d.h. wenn $\mathrm{ggT}(a, b) = 1$ gilt.

(2) Sind $a, b \in \mathbb{Z}$ teilerfremd, d.h. gilt $\mathrm{ggT}(a, b) = 1$, so gibt es Zahlen $u, v \in \mathbb{Z}$ mit
$$ua + vb = 1.$$
Setzt man $\widetilde{a} = ua$ und $\widetilde{b} = vb$, so gilt also
$$\widetilde{a} \in (a), \quad \widetilde{b} \in (b) \quad \text{und} \quad \widetilde{a} + \widetilde{b} = 1.$$
Zahlen u, v können mit dem erweiterten euklidischen Algorithmus bestimmt werden, manchmal funktioniert auch Probieren.

Satz (Chinesischer Restsatz). *Sei R ein kommutativer Ring und seien $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ paarweise teilerfremde Ideale, d.h. $\mathfrak{a}_i + \mathfrak{a}_j = R$ für alle $i \neq j$.*

(1) *Es gibt Elemente $a_{i,j} \in R$ mit*
$$a_{i,j} \in \mathfrak{a}_i \quad \textit{und} \quad a_{i,j} + a_{j,i} = 1 \textit{ für alle } i \neq j.$$

(2) *Definiert man für $i = 1, \ldots, n$*
$$b_i = \prod_{j \neq i} a_{j,i},$$
so gilt:
$$b_i \equiv 1 \bmod \mathfrak{a}_i \quad \textit{und} \quad b_i \equiv 0 \bmod \mathfrak{a}_j \textit{ für alle } j \neq i \quad \textit{und} \quad b_i \in \prod_{j \neq i} \mathfrak{a}_j.$$

(3) *Es gilt*
$$\prod_{i=1}^{n} \mathfrak{a}_i = \bigcap_{i=1}^{n} \mathfrak{a}_i.$$

(4) *Für beliebige $x_i \in R$ wird das Kongruenzgleichungssystem*

$$x \equiv \begin{cases} x_1 \bmod \mathfrak{a}_1, \\ \vdots \\ x_n \bmod \mathfrak{a}_n \end{cases}$$

gelöst durch

$$x = \sum_{i=1}^{n} b_i x_i$$

und die Lösung ist eindeutig modulo $\prod_{i=1}^n \mathfrak{a}_i = \bigcap_{i=1}^n \mathfrak{a}_i$.

Beweis:

(1) Dies folgt sofort aus $\mathfrak{a}_i + \mathfrak{a}_j = R$ für $i \neq j$.

(2) Wegen $a_{j,i} \in \mathfrak{a}_j$ gilt natürlich

$$b_i = \prod_{j \neq i} a_{j,i} \in \prod_{j \neq i} \mathfrak{a}_i.$$

Dann ist natürlich auch $b_i \in \mathfrak{a}_j$ für $j \neq i$ und damit

$$b_i \equiv 0 \bmod \mathfrak{a}_j \text{ für } j \neq i.$$

Wegen $a_{i,j} \in \mathfrak{a}_i$ gilt weiter

$$b_i = \prod_{j \neq i} a_{j,i} = \prod_{j \neq i} (1 - a_{i,j}) \equiv \prod_{j \neq i} 1 \equiv 1 \bmod \mathfrak{a}_i.$$

(3) Wir beweisen nun $\prod_{i=1}^n \mathfrak{a}_i = \bigcap_{i=1}^n \mathfrak{a}_i$. Die Inklusion $\subseteq$ ist klar. Wir müssen nur noch die Umkehrung zeigen. Wir beweisen dies durch Induktion nach n.

- **Fall $n = 1$:** Klar.
- **Fall $n = 2$:** Es ist $a_{1,2} + a_{2,1} = 1$. Ist $x \in \mathfrak{a}_1 \cap \mathfrak{a}_2$, so ist $xa_{1,2} \in \mathfrak{a}_1\mathfrak{a}_2$ und $xa_{2,1} \in \mathfrak{a}_1\mathfrak{a}_2$, also

$$x = xa_{1,2} + xa_{2,1} \in \mathfrak{a}_1\mathfrak{a}_2,$$

und damit $\mathfrak{a}_1 \cap \mathfrak{a}_2 \subseteq \mathfrak{a}_1\mathfrak{a}_2$, was wir zeigen wollten.
- **Fall $n \geq 3$:** Die Aussage sei bereits für $n-1$ bewiesen, d.h.

$$\mathfrak{b} = \bigcap_{i=1}^{n-1} \mathfrak{a}_i = \prod_{i=1}^{n-1} \mathfrak{a}_i.$$

Es ist

$$b_n = \prod_{j=1}^{n-1} a_{j,n} \in \prod_{i=1}^{n-1} \mathfrak{a}_i = \mathfrak{b}.$$

Modulo $\mathfrak{a}_n$ gilt

$$b_n = \prod_{j=1}^{n-1} (1 - a_{n,j}) \equiv 1 \bmod \mathfrak{a}_n,$$

also

$$1 \in (b_n) + \mathfrak{a}_n \in \mathfrak{b} + \mathfrak{a}_n, \quad \text{und damit} \quad \mathfrak{b} + \mathfrak{a}_n = R.$$

Wir können jetzt den Fall $n = 2$ auf $\mathfrak{b}$ und $\mathfrak{a}_n$ anwenden und erhalten:

$$\prod_{i=1}^{n} \mathfrak{a}_i = \prod_{i=1}^{n-1} \mathfrak{a}_i \cdot \mathfrak{a}_n = \mathfrak{b} \cdot \mathfrak{a}_n = \mathfrak{b} \cap \mathfrak{a}_n = \bigcap_{i=1}^{n-1} \mathfrak{a}_i \cap \mathfrak{a}_n = \bigcap_{i=1}^{n} \mathfrak{a}_i.$$

Damit ist die Behauptung durch Induktion bewiesen.

(4) Sind $x_i \in R$ vorgegeben, bilden wir

$$x = \sum_{i=1}^{n} b_i x_i,$$

schreiben wir

$$x = b_i x_i + \sum_{j \neq i} b_j x_j,$$

so folgt aus $b_i \equiv 1 \bmod \mathfrak{a}_i$ und $b_j \equiv 0 \bmod \mathfrak{a}_i$ (für $j \neq i$) sofort

$$x \equiv x_i \bmod \mathfrak{a}_i.$$

Dies zeigt, dass x das angegebene Kongruenzgleichungssystem löst. Für $y \in R$ gilt nun

$$\begin{aligned} y \equiv x_i \bmod \mathfrak{a}_i \text{ für alle } i \quad &\Longleftrightarrow \quad y \equiv x \bmod \mathfrak{a}_i \text{ für alle } i \quad \Longleftrightarrow \\ &\Longleftrightarrow \quad y - x \in \mathfrak{a}_i \text{ für alle } i \quad \Longleftrightarrow \\ &\Longleftrightarrow \quad y - x \in \bigcap_{i=1}^{n} \mathfrak{a}_i \quad \Longleftrightarrow \\ &\Longleftrightarrow \quad y \equiv x \bmod \bigcap_{i=1}^{n} \mathfrak{a}_i. \end{aligned}$$

Dies beweist, dass die Lösung eindeutig modulo $\bigcap_{i=1}^{n} \mathfrak{a}_i = \prod_{i=1}^{n} \mathfrak{a}_i$ ist. ■

Wir geben noch eine weitere Fassung des chinesischen Restsatzes an, die unmittelbar aus dem vorangegangenen Satz folgt. (Da Restklassen modulo verschiedener Ideale betrachtet werden, schreiben wir diese in der Mengenschreibweise $x + \mathfrak{a}$ etc.)

Satz. *Sei R ein kommutativer Ring und seien $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ paarweise verschiedene Ideale, d.h. $\mathfrak{a}_i + \mathfrak{a}_j = R$ für alle $i \neq j$. Dann gilt:*

(1) *Der kanonische Ringhomomorphismus*

$$\phi : R \to R/\mathfrak{a}_1 \times \cdots \times R/\mathfrak{a}_n, \quad x \mapsto (x + \mathfrak{a}_1, \ldots, x + \mathfrak{a}_n)$$

ist surjektiv mit Kern

$$\operatorname{Kern}(\phi) = \bigcap_{i=1}^{n} \mathfrak{a}_i = \prod_{i=1}^{n} \mathfrak{a}_i.$$

(2) *ϕ induziert einen Ringisomorphismus*

$$\overline{\phi} : R/\mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n \xrightarrow{\simeq} R/\mathfrak{a}_1 \times \cdots \times R/\mathfrak{a}_n \quad \text{bzw.} \quad \overline{\phi} : R/\mathfrak{a}_1 \ldots \mathfrak{a}_n \xrightarrow{\simeq} R/\mathfrak{a}_1 \times \cdots \times R/\mathfrak{a}_n.$$

(3) *Sind $b_1, \ldots, b_n \in R$ wie im vorangegangenen Satz, so ist*

$$\overline{\phi}^{-1}((x_1 + \mathfrak{a}_1, \ldots, x_n + \mathfrak{a}_n)) = (x_1 b_1 + \cdots + x_n b_n) + \mathfrak{a}_1 \ldots \mathfrak{a}_n.$$

Beispiel: Wir betrachten in $\mathbb{Z}$ das Kongruenzgleichungssystem vom Beginn des Abschnitts:

$$x \equiv \begin{cases} 8 \bmod 80, \\ 31 \bmod 81, \\ 66 \bmod 79. \end{cases}$$

Wir schreiben

$$\mathfrak{a}_1 = (80), \quad \mathfrak{a}_2 = (81), \quad \mathfrak{a}_3 = (79).$$

Wir wählen

$$a_{1,2} = -80, \quad a_{2,1} = 81, \quad a_{1,3} = 80, \quad a_{3,1} = -79.$$

Dann gilt

$$a_{1,2}, a_{1,3} \in \mathfrak{a}_1, \quad a_{2,1} \in \mathfrak{a}_2, \quad a_{3,1} \in \mathfrak{a}_3, \quad a_{1,2} + a_{2,1} = 1, \quad a_{1,3} + a_{3,1} = 1.$$

Um $\mathfrak{a}_2$ und $\mathfrak{a}_3$ zu vergleichen, dividieren wir mit Rest:

$$81 = 1 \cdot 79 + 2, \quad 79 = 39 \cdot 2 + 1,$$

woraus sich

$$1 = 79 - 39 \cdot 2 = 79 - 39 \cdot (81 - 79) = -39 \cdot 81 + 40 \cdot 79$$

ergibt. (Natürlich hätten wir auch den erweiterten euklidischen Algorithmus anwenden können.) Wir wählen also

$$a_{2,3} = -39 \cdot 81 = -3159, \quad a_{3,2} = 40 \cdot 79 = 3160$$

und haben dann

$$a_{2,3} \in \mathfrak{a}_2, \quad a_{3,2} \in \mathfrak{a}_3, \quad a_{2,3} + a_{3,2} = 1.$$

Nun bilden wir

$$\begin{aligned} b_1 &= a_{2,1}a_{3,1} = 81 \cdot (-79) = -6399, \\ b_2 &= a_{1,2}a_{3,2} = (-80) \cdot 3160 = -252800, \\ b_3 &= a_{1,3}a_{2,3} = 80 \cdot (-3159) = -252720. \end{aligned}$$

Damit ist eine Lösung des Kongruenzgleichungssystems

$$\widetilde{x} = 8b_1 + 31b_2 + 66b_3 = 8 \cdot (-6399) + 31 \cdot (-252800) + 66 \cdot (-252720) = -24567512.$$

Die Lösungen des Kongruenzgleichungssystems sind bestimmt modulo $80 \cdot 81 \cdot 79 = 511920$. Daher ist die kleinste positive Lösung $\widetilde{x}$ mod $80 \cdot 81 \cdot 79$, also

$$x = \widetilde{x} \bmod 511920 = 4648.$$

Beispiel: In $\mathbb{Z}[i]$ betrachten wir die Ideale

$$\mathfrak{a}_1 = (1 + 2i) \quad \text{und} \quad \mathfrak{a}_2 = (1 - 2i).$$

- Wir suchen zunächst nach Elementen $a_{1,2} \in \mathfrak{a}_1$ und $a_{2,1} \in \mathfrak{a}_2$ mit $a_{1,2} + a_{2,1} = 1$. Wegen $5 = (1 + 2i)(1 - 2i)$ gilt $5 \in \mathfrak{a}_1$ und $5 \in \mathfrak{a}_2$. Es ist

  $$(1 + 2i) + (1 - 2i) = 2, \quad \text{damit} \quad (-2 - 4i) + (-2 + 4i) = -4,$$

  also

  $$(5 - 2 - 4i) + (-2 + 4i) = 1.$$

  Nun ist

  $$3 - 4i = 5 - 2 \cdot (1 + 2i) \in \mathfrak{a}_1 \quad \text{und} \quad -2 + 4i = -2(1 - 2i) \in \mathfrak{a}_2.$$

  Setzen wir also

  $$a_{1,2} = 3 - 4i \quad \text{und} \quad a_{2,1} = -2 + 4i,$$

  so gilt

  $$a_{1,2} \in \mathfrak{a}_1, \quad a_{2,1} \in \mathfrak{a}_2 \quad \text{und} \quad a_{1,2} + a_{2,1} = 1.$$

  Insbesondere sind die Ideale $\mathfrak{a}_1$ und $\mathfrak{a}_2$ teilerfremd.
- Wir bilden nun wie im Satz

  $$b_1 = \prod_{j \le 1} a_{j,1} = a_{2,1} = -2 + 4i \quad \text{und} \quad b_2 = \prod_{j \ne 2} a_{j,2} = a_{1,2} = 3 - 4i.$$

- Ein Kongruenzgleichungssystem

  $$x \equiv x_1 \bmod \mathfrak{a}_1, \quad x \equiv x_2 \bmod \mathfrak{a}_2$$

  wird nun gelöst durch

  $$x = b_1x_1 + b_2x_2$$

  und ist eindeutig bestimmt modulo $\mathfrak{a}_1\mathfrak{a}_2$. Es gilt

  $$\mathfrak{a}_1\mathfrak{a}_2 = (1 + 2i)(1 - 2i) = (5).$$

- Wir betrachten das Gleichungssystem

  $$x \equiv 2 \bmod \mathfrak{a} \quad \text{und} \quad x \equiv 3 \bmod \mathfrak{b}.$$

  Wir berechnen also

  $$x = x_1b_1 + x_2b_2 = 2(-2 + 4i) + 3(3 - 4i) = 5 - 4i = i + 5(1 - i).$$

  Die betragsmäßig kleinste Lösung ist dann $x = i$.

9. Anhang: Das Zornsche Lemma und die Existenz maximaler Ideale

DEFINITION. *Eine Relation $\leq$ auf einer Menge M wird* **Ordnung** *(manchmal auch* **partielle Ordnung** *genannt, wenn folgende Eigenschaften erfüllt sind:*

- *Reflexivität: Es gilt $x \leq x$ für alle $x \in M$.*
- *Transitivität: Aus $x \leq y$ und $y \leq z$ folgt $x \leq z$.*
- *Antisymmetrie: Aus $x \leq y$ und $y \leq x$ folgt $x = y$.*

Beispiele:

(1) $\mathbb{R}$ mit der üblichen $\leq$-Relation ist eine Ordnung.
(2) $\mathbb{N}$ mit der Teilbarkeitsrelation $a \mid b$ ist eine Ordnung.
(3) Ist A eine Menge und $\mathfrak{P}(A)$ die Menge aller Teilmengen von A, so ist $\subseteq$ eine Ordnung auf $\mathfrak{P}(A)$.
(4) Sei R ein Ring und $\mathfrak{a} \subsetneq R$ ein Ideal. Sei
$$A = \{\mathfrak{b} \text{ Ideal in } R : \mathfrak{a} \subseteq \mathfrak{b} \subsetneq R\}$$
die Menge der von R verschiedenen Ideale von R, die $\mathfrak{a}$ enthalten. Dann definiert $\subseteq$ eine Ordnung auf A.

DEFINITION. *Sei $\leq$ eine Ordnung auf einer Menge M und A eine Teilmenge von M. Ein Element $b \in M$ heißt eine* **obere Schranke für** *A, wenn gilt:*
$$a \in A \quad \Longrightarrow \quad a \leq b.$$

Beispiel: Wir betrachten $\mathbb{R}$ der der üblichen $\leq$-Relation. Das Intervall $(0, 1)$ besitzt (viele) obere Schranken, beispielsweise 1. Die Teilmenge $\mathbb{N}$ besitzt keine obere Schranke.

DEFINITION. *Sei $\leq$ eine Ordnung auf einer Menge M. Eine Teilmenge $A \subseteq M$ heißt* **total geordnet**, *wenn folgende Implikation gilt:*
$$x, y \in A \quad \Longrightarrow \quad x \leq y \text{ oder } y \leq x.$$
(Zwei Elemente lassen sich also immer vergleichen.)

LEMMA. *Sei R ein Ring und $\mathfrak{a}$ ein von R verschiedenes Ideal. Sei $A = \{\mathfrak{b}$ Ideal in $R : \mathfrak{a} \subseteq \mathfrak{b} \subsetneq R\}$ mit $\subseteq$ geordnet. Sei B eine totalgeordnete, nichtleere Teilmenge von A. Dann ist*
$$\widetilde{\mathfrak{b}} = \bigcup_{\mathfrak{b} \in B} \mathfrak{b}$$
ein Ideal in R mit $\mathfrak{a} \subseteq \widetilde{\mathfrak{b}} \subsetneq R$, also $\widetilde{\mathfrak{b}} \in A$. Das Ideal $\widetilde{\mathfrak{b}}$ ist eine obere Schranke für B.

Beweis: Wir zeigen zunächst, dass $\widetilde{\mathfrak{b}}$ ein Ideal ist:

- Ist $\mathfrak{b} \in B$, so ist $0 \in \mathfrak{b}$, also $0 \in \widetilde{\mathfrak{b}}$.
- Seien $x, y \in \widetilde{\mathfrak{b}}$. Dann gibt es Ideale $\mathfrak{b}_x, \mathfrak{b}_y \in B$ mit $x \in \mathfrak{b}_x$ und $y \in \mathfrak{b}_y$. Da B totalgeordnet ist, gilt $\mathfrak{b}_x \subseteq \mathfrak{b}_y$ oder $\mathfrak{b}_y \subseteq \mathfrak{b}_x$. Sei also o.E. $\mathfrak{b}_x \subseteq \mathfrak{b}_y$. Dann ist auch $x \in \mathfrak{b}_y$, also $x + y \in \mathfrak{b}_y \subseteq \widetilde{\mathfrak{b}}$.
- Sei $r \in R$ und $x \in \widetilde{\mathfrak{b}}$. Dann gibt es ein Ideal $\mathfrak{b}_x \in B$ mit $x \in \mathfrak{b}_x$. Da $\mathfrak{b}_x$ ein Ideal ist, gilt $rx, xr \in \mathfrak{b}_x$, also $rx, xr \in \widetilde{\mathfrak{b}}$.

Daher ist $\widetilde{\mathfrak{b}}$ ein Ideal in R.
Warum gilt $\widetilde{\mathfrak{b}} \subsetneq R$. Wäre $\widetilde{\mathfrak{b}} = R$, so wäre $1 \in \widetilde{\mathfrak{b}}$, also gäbe es ein $\mathfrak{b} \in B$ mit $1 \in \mathfrak{b}$. Dann wäre aber $\mathfrak{b} = R$, ein Widerspruch. Also gilt $\widetilde{\mathfrak{b}} \neq R$.
Da natürlich $\mathfrak{a} \subseteq \widetilde{\mathfrak{b}}$ gilt, ist $\widetilde{\mathfrak{b}}$ in A, und damit eine obere Schranke für B. ■

DEFINITION. *Sei M eine Menge mit einer Ordnung $\leq$. Ein Element $m \in M$ heißt ein* **maximales Element**, *wenn folgende Implikation gilt:*
$$m \leq x \quad \Longrightarrow \quad m = x.$$

LEMMA (Zorn). *Ist M eine nichtleere Menge mit einer Ordnung $\leq$, in der jede nichtleere, totalgeordnete Teilmenge eine obere Schranke besitzt, so besitzt M (mindestens) ein maximales Element.*

SATZ. *Sei R ein Ring und $\mathfrak{a}$ ein von R verschiedenes Ideal. Dann gibt es ein maximales Ideal $\mathfrak{m}$, das $\mathfrak{a}$ enthält.*

Beweis: Wir betrachten $A = \{b \text{ Ideal in } R : \mathfrak{a} \subseteq \mathfrak{b} \subsetneq R\}$ mit $\subseteq$ als Ordnung. Im Lemma haben wir gesehen, dass jede nichtleere, totalgeordnete Teilmenge eine obere Schranke besitzt. Nach dem Zornschen Lemma enthält A ein maximales Element $\mathfrak{m}$. Wir wissen daher, dass $\mathfrak{m}$ ein Ideal ist mit $\mathfrak{a} \subseteq \mathfrak{m} \subsetneq R$. Sei nun $\mathfrak{c}$ irgendein Ideal von R mit

$$\mathfrak{m} \subsetneq \mathfrak{c} \subseteq R \quad .$$

Wäre $\mathfrak{c} \neq R$, so wäre $\mathfrak{c} \in A$; dann wäre aber $\mathfrak{m}$ nicht mehr maximal. Daher gilt $\mathfrak{c} = R$, was beweist, dass $\mathfrak{m}$ ein maximales Ideal ist.