1. Grundbegriffe der Ringtheorie

(1.1) Definition. *Ein* **Ring** *ist eine Menge R mit zwei Rechenoperationen*

$$\begin{array}{ccc} R\times R & \to & R \\ (a,b) & \mapsto & a+b \end{array} \quad \textit{und} \quad \begin{array}{ccc} R\times R & \to & R \\ (a,b) & \mapsto & a\cdot b \end{array}$$

(genannt **Addition** *und* **Multiplikation***), die die folgenden Bedingungen erfüllen:*

(1) $a+b=b+a$ *für alle* $a,b\in R$;
(2) $(a+b)+c=a+(b+c)$ *für alle* $a,b,c\in R$;
(3) *es gibt ein Element* $0\in R$ *mit* $a+0=a$ *für alle* $a\in R$;
(4) *zu jedem Element* $x\in R$ *gibt es ein Element* $-x\in R$ *mit* $x+(-x)=0$;
(5) $(a\cdot b)\cdot c=a\cdot(b\cdot c)$ *für alle* $a,b,c\in R$;
(6) $a\cdot(b+c)=(a\cdot b)+(a\cdot c)$ *für alle* $a,b,c\in R$.
(7) $(a+b)\cdot c=(a\cdot c)+(b\cdot c)$ *für alle* $a,b,c\in R$.

Gibt es zusätzlich zu (1)-(7) *ein Element* $1\in R$ *mit* $1\cdot a=a\cdot 1=a$ *für alle* $a\in R$*, so heißt* R *ein* **Ring mit Einselement** *oder* **unitärer Ring**. *Gilt zusätzlich zu* (1)-(7) *die Bedingung* $a\cdot b=b\cdot a$ *für alle* $a,b\in R$*, so heißt* R *ein* **kommutativer Ring**.

(1.2) Bemerkungen. (a) Statt $a\cdot b$ schreiben wir kurz ab. Wir verwenden ferner die Konvention "Punkt vor Strich", schreiben also kurz $ab+cd$ statt $(ab)+(cd)$.

(b) Die Definition eines Rings besagt, daß $(R,+)$ eine abelsche Gruppe und $(R,\cdot)$ eine Halbgruppe ist. Die Bedingungen (6) und (7), die man als **Distributivgesetze** bezeichnet, koppeln die Addition und die Multiplikation miteinander.

(c) Das Nullelement in (3) ist eindeutig bestimmt. Sind nämlich 0 und $0'$ Nullelemente, so gilt $0=0+0'=0'$.

(d) Das zu x additiv inverse Element $-x$ ist eindeutig bestimmt (sonst wäre $-x$ gar keine wohldefinierte Notation). Sind nämlich x_1 und x_2 additiv invers zu x, so gilt $x_2=x_2+0=x_2+(x+x_1)=(x_2+x)+x_1=0+x_1=x_1$.

(e) Es gilt $a\cdot 0=0$ für alle $a\in R$, denn es gilt $a\cdot 0=a\cdot(0+0)=a\cdot 0+a\cdot 0$, nach beiderseitiger Addition von $-(a\cdot 0)$ unter Ausnutzung von (2) also $0=a\cdot 0$. Vollkommen analog gilt $0\cdot a=0$ für alle $a\in R$.

(f) Besitzt ein Ring R ein Einselement, so ist dieses eindeutig bestimmt. Sind nämlich 1 und $1'$ Einselemente, so gilt $1=1\cdot 1'=1'$. Der Fall $1=0$ ist dabei nicht ausgeschlossen, kann aber nur für den trivialen Ring $R=\{0\}$ eintreten: ist nämlich $1=0$, dann auch $a=a\cdot 1=a\cdot 0=0$ für alle $a\in R$.

(1.3) Beispiele. (a) Die Menge $\mathbb{Z}$ aller ganzen Zahlen ist mit der üblichen Addition und Multiplikation ein kommutativer Ring mit Einselement.

(b) Die Menge $\mathbb{Z}_n$ aller Restklassen modulo n ist mit der üblichen Addition und Multiplikation modulo n ein kommutativer Ring mit Einselement. (Wir werden sehen, daß sich $\mathbb{Z}_n$ aus $\mathbb{Z}$ durch eine sehr allgemeine Konstruktion ergibt, nämlich den Übergang eines Ring R zu einem Quotientenring R/I.)

(c) Es sei $n\in\mathbb{Z}\setminus\{0,1\}$ eine quadratfreie ganze Zahl (also nicht teilbar durch eine von 1 verschiedene Quadratzahl). Dann ist die Menge $\mathbb{Z}+\mathbb{Z}\sqrt{n}:=\{a+b\sqrt{n}\mid a,b\in\mathbb{Z}\}$ mit den von $\mathbb{C}$ geerbten Rechenoperationen ein kommutativer Ring mit Einselement. Speziell für $n=-1$ erhalten wir den Ring $\mathbb{Z}+i\mathbb{Z}$; dessen Elemente heißen Gaußsche ganze Zahlen.

(d) Jeder Körper ist ein kommutativer Ring mit Einselement. Das gilt beispielsweise für die Körper $\mathbb{Q}\subseteq\mathbb{R}\subseteq\mathbb{C}$ oder auch die Restklassenringe $\mathbb{Z}_p$ mit p prim.

(e) Ist R ein Ring, so ist der Ring $R[X]$ aller formalen Polynome $a_0+a_1X+\cdots+a_nX^n$ mit Koeffizienten $a_i\in R$ ein Ring, wenn wir die üblichen Rechenregeln für Polynome verwenden.

(f) Allgemeiner können wir für einen gegebenen Ring R den Polynomring $R[(X_i)_{i\in I}]$ in einer beliebigen Menge $(X_i)_{i\in I}$ von (kommutierenden) Variablen einführen. Dieser ist definiert als die Menge aller endlichen formalen Summen $\sum_{i_k\in I,d_k\in\mathbb{N}_0} a_{i_1\dots i_r,d_1,\dots,d_r}X_{i_1}^{d_1}X_{i_2}^{d_2}\cdots X_{i_r}^{d_r}$ mit Koeffizienten in R. Es ist zweckmäßig die Konvention $X_{i_k}^0:=1$ zu verwenden. Genau dann ist $R[(X_i)_{i\in I}]$ unitär bzw. kommutativ, wenn R unitär bzw. kommutativ ist.

(g) Ist R ein Ring, so ist der Ring $R[[X]]$ aller formalen Potenzreihen $a_0+a_1X+a_2X^2+\cdots$ mit Koeffizienten $a_i\in R$ ein Ring, wenn wir die üblichen Rechenregeln für formale Potenzreihen verwenden.

(h) Allgemeiner können wir für einen gegebenen Ring R den Potenzreihenring $R[[(X_i)_{i\in I}]]$ in einer beliebigen Menge $(X_i)_{i\in I}$ von (kommutierenden) Variablen einführen. Dieser ist definiert als die Menge aller formalen Reihen der Form $\sum_{i_k\in I,d_k\in\mathbb{N}_0} a_{i_1\dots i_r,d_1,\dots,d_r}X_{i_1}^{d_1}X_{i_2}^{d_2}\cdots X_{i_r}^{d_r}$ mit Koeffizienten in R. Genau dann ist $R[[(X_i)_{i\in I}]]$ unitär bzw. kommutativ, wenn R unitär bzw. kommutativ ist.

(i) Es sei $(A,+)$ eine beliebige abelsche Gruppe. Dann können wir A zu einem kommutativen Ring machen, indem wir $xy:=0$ für alle $x,y\in A$ definieren. (Diese Multiplikation heißt die **triviale Multiplikation** auf A.)

(j) Ist R ein beliebiger Ring, so ist die Menge $R^{n\times n}$ aller $(n\times n)$-Matrizen mit der üblichen Definition der Addition und Multiplikation von Matrizen wieder ein Ring. Genau dann ist $R^{n\times n}$ unitär, wenn R unitär ist. Für $n\geq 2$ ist $R^{n\times n}$ genau dann kommutativ, wenn die Multiplikation in R trivial ist, wenn also $xy=0$ für alle $x,y\in R$ gilt. Gibt es nämlich Elemente $x,y\in R$ mit $xy\neq 0$, so gilt

$$\begin{bmatrix} x & 0\\ 0 & 0\end{bmatrix}\begin{bmatrix} 0 & y\\ 0 & 0\end{bmatrix}=\begin{bmatrix} 0 & xy\\ 0 & 0\end{bmatrix}\neq\begin{bmatrix} 0 & 0\\ 0 & 0\end{bmatrix}=\begin{bmatrix} 0 & y\\ 0 & 0\end{bmatrix}\begin{bmatrix} x & 0\\ 0 & 0\end{bmatrix}.$$

(k) Sind R ein beliebiger Ring und $X\neq\emptyset$ eine beliebige Menge, so wird die Menge $R^X:=\{f:X\to R\}$ aller Funktionen von X nach R zu einem Ring, indem wir Addition und Multiplikation argumentweise definieren, also durch $(f+g)(x):=f(x)+g(x)$ und $(f\cdot g)(x):=f(x)g(x)$.

(l) Ist $(A,+)$ eine beliebige abelsche Gruppe, so wird die Menge A^A aller Funktionen $f:A\to A$ zu einem Ring

R, wenn wir als Rechenoperationen die argumentweise definierte Addition $(f+g)(a) := f(a)+g(a)$ und die Verkettung $(f \circ g)(a) := f\big(g(a)\big)$ wählen. Der Ring R ist unitär (mit der identischen Abbildung als Einselement), aber für $A \neq \{0\}$ nicht kommutativ.

(m) Die Menge aller integrierbaren stetigen Funktionen $f : \mathbb{R} \to \mathbb{R}$ wird zu einem Ring, wenn wir die Addition punktweise definieren (also durch $(f+g)(x) := f(x)+g(x)$ für alle $x \in \mathbb{R}$) und die Multiplikation durch $(f \star g)(x) := \int_{-\infty}^{\infty} f(x-y)g(y)\mathrm{d}y$. (Die Operation $\star$ wird als **Faltung** bezeichnet.) In der Analysis wird gezeigt, daß dieser Ring kommutativ ist, aber kein Einselement besitzt. Eine Variante eines solchen Faltungsrings erhalten wir, wenn wir die Menge aller stetigen integrierbaren Funktionen $f : [0,\infty) \to \mathbb{R}$ betrachten und die Addition wieder punktweise, die Multiplikation aber durch $(f \star g)(x) := \int_0^x f(x-y)g(y)\mathrm{d}y$ definieren.

(n) Sind R und S Ringe, so können wir das kartesische Produkt $R \times S$ wieder zu einem Ring machen, indem wir Addition und Multiplikation definieren durch $(r_1,s_1)+(r_2,s_2) := (r_1+r_2, s_1+s_2)$ und $(r_1,s_1)\cdot(r_2,s_2) := (r_1s_1, r_2s_2)$. Der so erhaltene Ring heißt **direktes Produkt** von R und S.

(o) Allgemeiner sei $(R_i)_{i\in I}$ eine beliebige Familie von Ringen. Dann wird die Menge $\prod_{i\in I} R_i$ aller "Tupel" $(r_i)_{i\in I}$ (also aller Abbildungen $r : I \to \bigcup_{i\in I} R_i$ mit $r(i_0) \in R_{i_0}$ für alle i_0) zu einem Ring, wenn wir Addition und Multiplikation argumentweise definieren, also durch $(r_i)+(s_i) := (r_i+s_i)$ und $(r_i)\cdot(s_i) := (r_is_i)$. Mit diesen Operationen bezeichnet man $\prod_{i\in I} R_i$ als **direktes Produkt** der Ringe R_i. Genau dann ist R unitär bzw. kommutativ, wenn jeder einzelne der Ringe R_i unitär bzw. kommutativ ist.

(1.4) Definition. *Es sei R ein Ring.*

(a) *Ein Element $x \in R \setminus \{0\}$ heißt* **Nullteiler***, wenn es ein Element $y \neq 0$ in R gibt mit $xy = 0$ oder $yx = 0$.*

(b) *Ein Element $x \in R$ heißt* **nilpotent***, wenn es eine Zahl $n \in \mathbb{N}$ gibt mit $x^n = 0$.*

(c) *Ein Element $x \in R$ mit $x^2 = x$ heißt* **idempotent***.*

(1.5) Bemerkungen. (a) Jedes nilpotente Element $x \neq 0$ ist ein Nullteiler. Ist nämlich $n > 1$ die kleinste Zahl mit $x^n = 0$, so gilt $0 = x \cdot x^{n-1} = x^{n-1} \cdot x$ mit $x^{n-1} \neq 0$.

(b) Ist R unitär und ist $e \in R$ idempotent, dann auch $1-e$, denn aus $e^2 = e$ folgt $(1-e)^2 = 1-2e+e^2 = 1-2e+e = 1-e$. Die Elemente e und $1-e$ sind nun (außer in dem Trivialfall $R = \{0\}$) verschieden, denn aus $e = 1-e$ würde nach Multiplikation mit e die Gleichung $e^2 = e-e^2$ folgen; diese bedeutet aber $e = e-e = 0$ und damit $0 = e = 1-e = 1-0 = 1$. Also treten (außer für $R = \{0\}$) idempotente Elemente immer in Paaren auf.

(1.6) Definition. *Es sei R ein Ring mit dem Einselement 1. Ein Element $x \in R$ heißt* **invertierbares Element** *oder* **Einheit***, wenn es ein Element $y \in R$ gibt mit $xy = yx = 1$.*

(1.7) Bemerkungen. (a) Besitzt x ein linksinverses Element y_1 und ein rechtsinverses Element y_2, so sind diese zwangsläufig gleich (so daß x eine Einheit ist), denn aus $y_1x = 1$ und $xy_2 = 1$ folgt $y_1 = y_1 \cdot 1 = y_1(xy_2) = (y_1x)y_2 = 1 \cdot y_2 = y_2$. Da *jedes* linksinverse Element zu x mit *jedem* rechtsinversen Element zu x übereinstimmt, gibt es zu jeder Einheit x also *genau* ein Element y mit $xy = yx = 1$. Wir schreiben $y = x^{-1}$ und nennen y **(multiplikativ) invers** zu x.

(b) Wegen $1 \cdot 1 = 1$ ist 1 eine Einheit. Sind ferner x und y Einheiten, dann auch xy (denn es gilt $(xy)(y^{-1}x^{-1}) = x(yy^{-1})x^{-1} = x \cdot 1 \cdot x^{-1} = x \cdot x^{-1} = 1$, also $(xy)^{-1} = y^{-1}x^{-1}$). Damit bilden die Einheiten eines unitären Rings R eine multiplikative Gruppe; diese heißt die **Einheitengruppe** von R und wird mit $R^\times$ bezeichnet.

(c) Ein Ringelement kann nicht gleichzeitig Einheit und Nullteiler sein. Aus $xy_1 = 1$ und $y_2x = 0$ folgt nämlich $y_2 = y_2 \cdot 1 = y_2 \cdot (xy_1) = (y_2x) \cdot y_1 = 0 \cdot y_1 = 0$. Analog folgt aus $y_1x = 1$ und $xy_2 = 0$ schon $y_2 = 1 \cdot y_2 = (y_1x) \cdot y_2 = y_1 \cdot (xy_2) = y_1 \cdot 0 = 0$.

(1.8) Beispiele. (a) Es gilt $\mathbb{Z}^\times = \{\pm 1\}$.
(b) Es gilt $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$.
(c) Es gilt $\mathbb{Z}_n^\times = \{[x] \mid x \text{ teilerfremd zu } n\}$.
(d) Für einen Körper K gilt $K^\times = K \setminus \{0\}$.

(1.9) Beispiele. Der Ring R sei kommutativ und besitze ein Einselement. Dann gelten die folgenden Aussagen. (Beweise als Übungsaufgaben!)

(a) Die Einheitengruppe $(R^{n\times n})^\times$ des Matrizenrings $R^{n\times n}$ besteht genau aus denjenigen Matrizen $A \in R^{n\times n}$, für die $\det(A)$ in $R^\times$ liegt. (Was bedeutet das, wenn R ein Körper ist? Was bedeutet das im Fall $R = \mathbb{Z}$?)

(b) Die Einheitengruppe $R[X]^\times$ des Polynomrings $R[X]$ besteht genau aus denjenigen Polynomen $a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$, für die das Element a_0 eine Einheit in R ist und die Elemente $a_1, \ldots, a_n \in R$ nilpotent sind.

(c) Die Einheitengruppe $R[[X]]^\times$ des Potenzreihenrings $R[[X]]$ besteht genau aus denjenigen formalen Potenzreihen $a_0 + a_1X + a_2X^2 + \cdots$, für die das Element a_0 eine Einheit in R ist.

(1.10) Definition. *Ein Ring R heißt* **Integritätsbereich***, wenn er kommutativ und unitär ist und keine Nullteiler besitzt. Ein Ring R heißt* **Körper***, wenn er ein Integritätsbereich ist und wenn jedes von Null verschiedene Element invertierbar ist, wenn also $R^\times = R \setminus \{0\}$ gilt.*

(1.11) Beispiele. Die Ringe $\mathbb{Z}$ und $\mathbb{Z} + \mathbb{Z}\sqrt{2}$ sind Integritätsbereiche, aber keine Körper. Die Ringe $\mathbb{Q}$, $\mathbb{Q} + \mathbb{Q}\sqrt{2}$, $\mathbb{R}$ und $\mathbb{C}$ sind Körper.

(1.12) Definition. *Es sei R ein Ring. Eine Teilmenge $U \subseteq R$ heißt ein* **Unterring** *oder* **Teilring** *von R, wenn die folgenden Bedingungen gelten:*

(1) $U + U \subseteq U$, *d.h. für alle* $a, b \in U$ *gilt* $a + b \in U$;
(2) $0 \in U$;
(3) $-U \subseteq U$, *d.h., für alle* $a \in U$ *gilt* $-a \in U$;
(4) $U \cdot U \subseteq U$; *d.h., für alle* $a, b \in U$ *gilt* $ab \in U$.

Ist U ein Unterring von R, so schreiben wir $U \leq R$. Besitzt R ein Einselement 1, so heißt ein Unterring U von R ein **unitärer Unterring** *von R, wenn $1 \in U$ gilt.*

Offenbar ist U genau dann ein Unterring von R, wenn U mit den von R induzierten Rechenoperationen selbst ein Ring ist.

(1.13) Beispiele. (a) In der Folge $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ ist jeder Ring ein Unterring des Nachfolgers. Gleiches gilt für die Folge $\mathbb{Z} \subseteq \mathbb{Z} + i\mathbb{Z} \subseteq \mathbb{Q} + i\mathbb{Q} \subseteq \mathbb{C}$.

(b) Für jede feste Zahl $m \in \mathbb{Z}$ ist die Menge $m\mathbb{Z} = \{mx \mid x \in \mathbb{Z}\}$ aller Vielfachen von m ein Unterring von $\mathbb{Z}$.

(c) Es sei R ein beliebiger Ring. Indem wir ein Element r von R mit dem konstanten Polynom $r + 0 \cdot X + \cdots + 0 \cdot X^n$ identifizieren, können wir R als Unterring von $R[X]$ auffassen. Indem wir ein Polynom $a_0 + a_1X + \cdots + a_nX^n$ mit der endlichen Potenzreihe $a_0 + a_1X + \cdots + a_nX^n + 0 \cdot X^{n+1} + 0 \cdot X^{n+2} + \cdots$ identifizieren, können wir $R[X]$ als Unterring von $R[[X]]$ auffassen. Allgemeiner gilt

$$R \ \subseteq \ R[(X_i)_{i \in I}] \ \subseteq \ R[[(X_i)_{i \in I}]].$$

(d) Es seien R ein beliebiger Ring und $R^{n \times n}$ der Ring aller $(n \times n)$-Matrizen mit Koeffizienten in R. Die Menge aller oberen Dreiecksmatrizen (also aller Matrizen (r_{ij}) mit $r_{ij} = 0$ für $i > j$) ist dann ein Unterring von $R^{n \times n}$.

(e) Für ein Intervall $I \subseteq \mathbb{R}$ bezeichnen wir mit $C^k(I)$ die Menge aller k-mal stetig differentiierbaren Funktionen $f : I \to \mathbb{R}$. Dann ist $C^k(I)$ ein Unterring des Rings aller Funktionen $f : I \to \mathbb{R}$ (jeweils mit den argumentweise definieren Rechenoperationen).

(f) Jeder Ring R besitzt die trivialen Unterringe $U = \{0\}$ und $U = R$.

(g) Ist R ein beliebiger Ring, so ist das **Zentrum**

$$Z(R) \ := \ \{r \in R \mid rx = xr \text{ für alle } x \in R\}$$

ein Unterring von R. (Genau dann ist R kommutativ, wenn $Z(R) = R$ gilt.)

(h) Ist $(U_i)_{i \in I}$ eine beliebige Familie von Unterringen eines Rings R, so sind auch der Durchschnitt $\bigcap_{i \in I} U_i$ und die Summe $\sum_{i \in I} U_i$ Unterringe von R. Die Summe ist dabei definiert durch

$$\sum_{i \in I} U_i := \{u_{i_1} + \cdots + u_{i_n} \mid n \in \mathbb{N}, i_1, \ldots, i_n \in I, u_{i_k} \in U_{i_k}\}.$$

(i) Es sei $R = \prod_{i \in I} R_i$ das direkte Produkt von Ringen R_i. Für jede Teilmenge $J \subseteq I$ ist dann $\{(r_i)_{i \in I} \mid r_i = 0 \text{ für } i \notin J\}$ ein Unterring von R. Ferner ist die Menge aller Elemente $(r_i)_{i \in I}$, für die nur endlich viele Komponenten r_i von Null verschieden sind, ein Unterring von R; dieser wird die **direkte Summe** der Ringe R_i genannt und mit $\bigoplus_{i \in I} R_i$ bezeichnet.

Wir führen nun Ideale als spezielle Unterringe ein. In der Ringtheorie spielen Ideale gegenüber beliebigen Unterringen in etwa die gleiche Rolle wie in der Gruppentheorie Normalteiler gegenüber beliebigen Untergruppen.

(1.14) Definition. *Es sei R ein Ring. Ein Unterring $I \subseteq R$ heißt ein* **(zweiseitiges) Ideal***, wenn die Bedingungen $RI \subseteq I$ und $IR \subseteq I$ gelten, wenn also für alle $r \in R$ und alle $x \in I$ die Elemente rx und xr wieder in I liegen. In diesem Fall schreiben wir $I \trianglelefteq R$.*

(1.15) Beispiele. (a) Ist R ein beliebiger Ring, so sind $\{0\}$ und R Ideale von R. (Diese bezeichnet man als **triviale Ideale** von R.) Enthält in einem unitären Ring ein Ideal I auch nur ein einziges invertierbares Element x, so gilt schon $I = R$ (denn für $a \in R$ gilt dann $a = (ax^{-1})x \in ax^{-1}I \subseteq I$).

(b) Die Ideale von $\mathbb{Z}$ sind genau die Mengen der Form $\langle\langle d \rangle\rangle := \mathbb{Z}d = \{md \mid m \in \mathbb{Z}\}$ mit $d \in \mathbb{N}_0$.

(c) Für alle $a_1, \ldots, a_n \in R$ ist $\{p \in R[X_1, \ldots, X_n] \mid p(a_1, \ldots, a_n) = 0\}$ ein Ideal von $R[X_1, \ldots, X_n]$.

(d) Für jede Familie (R_i) von Ringen ist $\bigoplus_i R_i$ ein Ideal von $\prod_i R_i$.

(e) Für jede Familie $(I_\alpha)_{\alpha \in A}$ von Idealen von R ist der Durchschnitt $\bigcap_\alpha I_\alpha$ wieder ein Ideal von R.

(f) Es seien R ein Ring und $X \subseteq R$ eine beliebige Teilmenge von R. Dann gibt es ein eindeutig bestimmtes kleinstes Ideal I von R, das X umfaßt, nämlich den Durchschnitt aller Ideale von R, die X umfassen (von denen es mindestens eines gibt, nämlich R selbst). Wir bezeichnen I als von X **erzeugtes Ideal** und schreiben $I = \langle\langle X \rangle\rangle$. Ist $X = \{x_1, \ldots, x_n\}$ endlich, so schreiben wir auch $I = \langle\langle x_1, \ldots, x_n \rangle\rangle$. Ist R kommutativ, so gilt $I = Rx_1 + \cdots + Rx_n = \{a_1x_1 + \cdots + a_nx_n \mid a_i \in R\}$.

(g) Ein Ideal, das von einem einzigen Element erzeugt wird, bezeichnet man als **Hauptideal**. Beispiel (b) zeigt, daß im Ring R aller ganzen Zahlen jedes Ideal ein Hauptideal ist. Ein Ring mit dieser Eigenschaft heißt **Hauptidealring**.

(h) Ist K ein beliebiger Körper, so ist der Polynomring $K[X]$ ein Hauptidealring. Ist nämlich $I \neq \{0\}$ ein beliebiges Ideal und ist p ein Polynom minimalen Grades in I, so gilt $I = \langle\langle p \rangle\rangle$, wie Polynomdivision mit Rest zeigt.

(i) Ist $\mathfrak{I}$ eine totalgeordnete Menge von Idealen eines Rings R (gilt also $I \subseteq J$ oder $J \subseteq I$ für je zwei Ideale in $\mathfrak{I}$), so ist die Vereinigung $\bigcup \mathfrak{I}$ wieder ein Ideal von R.

(1.16) Definition. *Ein Ideal I eines Rings R heißt* **maximales Ideal***, wenn $I \neq R$ gilt und wenn es kein Ideal M gibt mit $I \subsetneqq M \subsetneqq R$.*

(1.17) Satz. *Es sei I ein Ideal des Rings R. Dann ist durch*

$$a \sim b \ :\Leftrightarrow \ a - b \in I$$

eine Äquivalenzrelation auf R erklärt. Die Äquivalenzklasse eines Elements $a \in R$ unter dieser Äquivalenzrelation

ist

$$[a] \;:=\; a+I \;=\; \{a+x \mid x \in I\}.$$

Die Menge aller dieser Äquivalenzklassen wird selbst zu einem Ring, wenn wir die Addition und die Multiplikation definieren durch

$$[a]+[b] := [a+b] \quad \textit{und} \quad [a]\cdot[b] := [ab].$$

Dieser Ring heißt **Faktorring** *oder* **Quotientenring** *von R modulo I und wird mit dem Symbol R/I bezeichnet.*

Beweis: Routinerechnung. ∎

(1.18) Beispiele. (a) Der Restklassenring $\mathbb{Z}_n$ ist nichts anderes als der Quotientenring von $\mathbb{Z}$ modulo des Ideal $n\mathbb{Z}$, also $\mathbb{Z}_n = \mathbb{Z}/(n\mathbb{Z})$.

(b) Es sei R ein unitärer kommutativer Ring. Dann ist I genau dann ein maximales Ideal, wenn R/I ein Körper ist. Die Bedingung, daß R/I ein Körper ist, daß also jedes Element $[a] \neq [0]$ in R/I invertierbar ist, bedeutet nämlich genau, daß es zu jedem Element $a \in R \setminus I$ Elemente $x \in I$ und $r \in R$ gibt mit $x + ra = 1$, daß also $I + Ra = R$ für alle $a \in R \setminus I$ gilt, und diese Bedingung drückt gerade die Maximalität des Ideals I aus.

Es gibt viele Möglichkeiten, aus schon bekannten Idealen neue zu konstruieren. Die wichtigsten dieser Möglichkeiten sind in der folgenden Definition angegeben. (Die Nachweise, daß die angegebenen Konstruktionen jeweils wieder ein Ideal liefern, seien als Übungsaufgaben empfohlen.)

(1.19) Definition und Satz. *Es sei R ein Ring. Dann liefern die folgenden Konstruktionen Ideale von R:*

(a) *der* **Durchschnitt** $\bigcap_{\alpha\in A} I_\alpha$ *einer beliebigen Familie $(I_\alpha)_{\alpha\in A}$ von Idealen;*

(b) *die* **Summe** $\sum_{\alpha\in A} I_\alpha$ *einer beliebigen Familie $(I_\alpha)_{\alpha\in A}$ von Idealen, die definiert ist als die Menge aller (endlichen) Summen $x_{\alpha_1} + \cdots + x_{\alpha_n}$ mit $\alpha_k \in A$ und $x_{\alpha_k} \in I_{\alpha_k}$;*

(c) *das* **Produkt** $I_1 I_2 \cdots I_n$ *endlich vieler Ideale $I_1, \ldots, I_n$, das definiert ist als die Menge aller Summen von Produkten der Form $x_1 x_2 \cdots x_n$ mit $x_k \in I_k$ für $1 \leq k \leq n$;*

(d) *die* **Potenz** I^n *eines Ideals I (mit $n \in \mathbb{N}$), die definiert ist als das n-fache Produkt $I \cdot I \cdots I$ (wobei man noch $I^0 := \langle\langle 1 \rangle\rangle = R$ setzt);*

(e) *der* **Quotient** $(I : J) := \{x \in R \mid xJ \subseteq I\}$ *zweier Ideale I und J;*

(f) *falls R kommutativ ist: das* **Radikal** *eines Ideals I, das definiert ist durch* $\mathrm{Rad}(I) := \sqrt{I} := \{x \in R \mid x^n \in I \text{ für ein } n \in \mathbb{N}\}$.

(1.20) Definition. *Eine Abbildung $f : R \to S$ zwischen zwei Ringen heißt ein* **Ringhomomorphismus**, *wenn sie die folgenden Bedingungen erfüllt:*

(1) $f(a+b) = f(a) + f(b)$ *für alle $a, b \in R$;*

(2) $f(ab) = f(a)f(b)$ *für alle $a, b \in R$.*

Wir nennen $f(R) := \{f(x) \mid x \in R\}$ das **Bild** *von f und* $\mathrm{Kern}(f) := \{x \in R \mid f(x) = 0\}$ *den* **Kern** *von f. Ein Ringhomomorphismus heißt* **Ringisomorphismus**, *wenn er bijektiv ist; in diesem Fall ist automatisch f^{-1} ebenfalls ein Ringisomorphismus. Sind R und S unitäre Ringe, so nennt man eine Abbildung $f : R \to S$ einen* **Homomorphismus unitärer Ringe**, *wenn außer* (1) *und* (2) *zusätzlich noch die Bedingung $f(1_R) = 1_S$ erfüllt ist.*

(1.21) Bemerkungen. (a) Streng genommen müßte man, um Ringhomomorphismen als strukturerhaltende Abbildungen zu definieren, auch noch die folgenden Bedingungen fordern: $f(0_R) = 0_S$ (Erhaltung des additiven Neutralelements), $f(-x) = -f(x)$ für alle $x \in R$ (Erhaltung additiver Inverser). Diese folgen aber schon aus den Bedingungen (1) und (2) (Übungsaufgabe!) und wurden daher nicht in die Definition mit aufgenommen.

(b) Ähnlich müßte man man einen Ringisomorphismus als eine Bijektion f zwischen Ringen definieren, für die sowohl f als auch f^{-1} ein Ringhomomorphismus ist. Da jeder bijektive Ringhomomorphismus automatisch diese Eigenschaft hat (Übungsaufgabe!), wurde die Definition schwächer formuliert.

(c) Einen Ringisomorphismus $f : R \to S$ darf man sich einfach vorstellen als Umbenennung der Elemente von R (nämlich $f(r)$ statt r), ohne irgendetwas an den algebraischen Beziehungen zwischen den einzelnen Elementen zu ändern. Isomorphe Ringe sind also sozusagen "gleich" (bis auf Umbenennen der Elemente).

(d) Sind $f : R \to S$ und $g : S \to T$ Ringhomomorphismen, so ist auch die Hintereinanderausführung $g \circ f : R \to T$ ein Ringhomomorphismus.

(e) Ist $f : R \to S$ ein Ringhomomorphismus, so ist $\mathrm{Kern}(f)$ ein Ideal von R.

(1.22) Beispiele. (a) Ist I ein Ideal des Rings R, so ist die Abbildung $R \to R/I$ mit $x \mapsto [x]$ ein Ringhomomorphismus. Ein Beispiel dafür ist die Abbildung $\mathbb{Z} \to \mathbb{Z}_n$, die (bei fest vorgegebenem n) jeder Zahl $x \in \mathbb{Z}$ ihre Restklasse $[x]$ modulo n zuordnet.

(b) Es seien R ein kommutativer Ring und $a_1, \ldots, a_n$ fest vorgegebene Ringelemente. Dann ist ein Ringhomomorphismus $\Phi : R[X_1, \ldots, X_n] \to R$ gegeben durch $\Phi(p) := p(a_1, \ldots, a_n)$. Man nennt Φ den **Auswertungshomomorphismus** an der Stelle $(a_1, \ldots, a_n) \in R^n$.

(c) Es seien $\varphi_1, \ldots, \varphi_m$ Polynome in n Variablen über einem Körper K. Dann ist ein Ringhomomorphismus $\Phi : K[X_1, \ldots, X_m] \to K[Y_1, \ldots, Y_n]$ gegeben durch

$$(\Phi p)(Y_1, \ldots, Y_n) := p\big(\varphi_1(Y_1, \ldots, Y_n), \ldots, \varphi_m(Y_1, \ldots, Y_n)\big).$$

Jede solche Abbildung heißt **Einsetzungshomomorphismus**, denn für die Variable X_i wird der Ausdruck $\varphi_i(Y_1, \ldots, Y_n)$ eingesetzt. Beispielsweise kann einem Polynom $p \in K[X, Y]$ in zwei Variablen ein Polynom $\widehat{p} = \Phi(p)$ in einer Variablen zugeordnet werden, indem man $\widehat{p}(T) := p(T^4 + T^2, T^3 - T)$ definiert (also $T^4 + T^2$ für X und $T^3 - T$ für Y einsetzt.

(1.23) Homomorphiesatz. *Es sei $\varphi : R \to S$ ein Ringhomomorphismus. Dann ist*

$$\Phi : \begin{array}{ccc} R/\mathrm{Kern}(\varphi) & \mapsto & \varphi(R) \\ [x] & \mapsto & \varphi(x) \end{array}$$

ein wohldefinierter Ringisomorphismus.

Beweis. Zunächst ist Φ wohldefiniert, denn aus $[x_1] = [x_2]$ folgt $[0] = [x_1 - x_2]$ und damit $x_1 - x_2 \in \mathrm{Kern}(\varphi)$, so daß $\varphi(x_1) = \varphi(x_2)$ gilt. Nun ist φ ein Ringhomomorphismus; also auch Φ. Da Φ von vornherein als Abbildung in den Ring $\varphi(R)$ aufgefaßt wird, ist Φ trivialerweise surjektiv. Aber Φ ist auch injektiv, denn aus $\Phi([x_1]) = \Phi([x_2])$, also $\varphi(x_1) = \varphi(x_2)$, folgt $x_1 - x_2 \in \mathrm{Kern}(\varphi)$ und damit $[x_1] = [x_2]$. ∎

Es ist zuweilen bequem, $x \equiv y$ modulo I statt $x - y \in I$ zu schreiben; wir sagen dann, die Ringelemente x und y seien kongruent modulo I. Der folgende Satz macht eine Aussage über das simultane Lösen mehrerer Kongruenzen modulo verschiedener Ideale eines Rings.

(1.24) Chinesischer Restsatz. *Es seien $I_1, \ldots, I_n$ Ideale eines Rings R, die die folgenden Bedingungen erfüllen:*

(1) *$R^2 + I_k = R$ für alle k;*
(2) *$I_i + I_j = R$ für alle $i \neq j$.*

(Beachte, daß (1) automatisch erfüllt ist, wenn R ein Einselement besitzt, denn dann gilt ja sogar $R^2 = R$.) Ferner seien $x_1, \ldots, x_n$ beliebige Elemente von R. Dann gibt es ein Element $x \in R$ mit $x \equiv x_i$ modulo x_i für $1 \leq i \leq n$, und die Abbildung

$$\begin{array}{ccc} R/(I_1 \cap \cdots \cap I_n) & \to & (R/I_1) \times \cdots \times (R/I_n) \\ [x]_I & \mapsto & ([x]_{I_1}, \ldots, [x]_{I_n}) \end{array}$$

ist ein Ringisomorphismus.

Beweis. Wir haben

$$R \;=\; I_1 + R^2 \;=\; I_1 + (I_1 + I_2)(I_1 + I_3) \;\subseteq\; I_1 + I_2 I_3,$$

folglich

$$R \;=\; I_1 + R^2 \;\subseteq\; I_1 + (I_1 + I_2 I_3)(I_1 + I_4) \;\subseteq\; I_1 + I_2 I_3 I_4$$

und so weiter, insgesamt also $R = I_1 + I_2 I_3 \cdots I_n \subseteq I_1 + I_2 \cap I_3 \cap \cdots \cap I_n \subseteq R$. Die gleiche Überlegung können wir statt mit I_1 mit jedem anderen der Ideale I_k durchführen; für $1 \leq k \leq n$ gilt also

$$(\star) \qquad R \;=\; I_k + \bigcap_{j \neq k} I_j.$$

Nun seien $r_1, \ldots, r_n \in R$ beliebig vorgegeben. Wegen $(\star)$ gibt es Elemente $a_k \in I_k$ und $b_k \in \bigcap_{j \neq k} I_j$ mit $r_k = a_k + b_k$. Für $r := b_1 + \cdots + b_n$ gilt dann $r \equiv b_k \equiv r_k$ modulo I_k. Da $r_1, \ldots, r_n \in R$ beliebig waren, ist damit gezeigt, daß der Ringhomomorphismus

$$\varphi : \begin{array}{ccc} R & \to & (R/I_1) \times \cdots \times (R/I_n) \\ r & \mapsto & ([r]_{I_1},\ \ldots,\ [r]_{I_n}) \end{array}$$

surjektiv ist. Nach dem Homomorphiesatz ist dann die auf $R/\mathrm{Kern}(\varphi)$ induzierte Abbildung ein Isomorphismus. Wegen $\mathrm{Kern}(\varphi) = I_1 \cap \cdots \cap I_n$ ist dies gerade die Behauptung. ∎

(1.25) Beispiel. Wir wollen alle Zahlen $x \in \mathbb{Z}$ finden, die simultan die Kongruenzen $x \equiv 1$ modulo 2, $x \equiv 2$ modulo 3 und $x \equiv 3$ modulo 5 erfüllen. Dazu wenden wir den Chinesischen Restsatz mit

$$I_1 := 2\mathbb{Z}, \quad I_2 := 3\mathbb{Z}, \quad I_3 := 5\mathbb{Z}$$

an. Gemäß dem Beweis dieses Satzes suchen wir Zahlen $a_i, b_i \in \mathbb{Z}$, die die folgenden Bedingungen erfüllen:

$1 = a_1 + b_1$ mit $a_1 \in I_1 = 2\mathbb{Z}$ und $b_1 \in I_2 \cap I_3 = 15\mathbb{Z}$,
$2 = a_2 + b_2$ mit $a_2 \in I_2 = 3\mathbb{Z}$ und $b_2 \in I_1 \cap I_3 = 10\mathbb{Z}$,
$3 = a_3 + b_3$ mit $a_3 \in I_3 = 5\mathbb{Z}$ und $b_3 \in I_1 \cap I_2 = 6\mathbb{Z}$.

Mit scharfem Hinschauen (oder systematischem Anwenden des Euklidischen Algorithmus) erhält man die Lösungen $(a_1, b_1) = (16, -15)$, $(a_2, b_2) = (-18, 20)$ und $(a_3, b_3) = (-15, 18)$. Dann ist $x := b_1 + b_2 + b_3 = 23$ eine Lösung der Aufgabe, und jede andere Lösung unterscheidet sich von dieser um ein Vielfaches von $2 \cdot 3 \cdot 5 = 30$. Es sind also genau die Zahlen der Form $23 + 30k$ mit $k \in \mathbb{Z}$, die die angegebenen Kongruenzen simultan erfüllen.