Auch wenn die Isomorphiesätze im Moment noch sehr technisch aussehen und etwas Zeit zum Verdauen der Beweise notwendig ist, so sind diese doch ganz zentrale Aussagen der Algebra. Sie verbinden Aussagen über Faktorringe mit Aussagen über Bilder von Ringhomomorphismen. In der Praxis ist es bisweilen wesentlich einfacher, einen Kern eines Homomorphismus auszurechnen als das Bild; aber dank des Homomorphiesatzes kennt man dann auch das Bild bis auf Isomorphie. Der erste Isomorphiesatz erleichtert das Arbeiten in Unterringen und deren Faktorringen oft wesentlich, während der zweite Isomorphiesatz den problemlosen Umgang mit Faktorringen von Faktorringen erlaubt.

4.6 Primideale und maximale Ideale

Im vorigen Kapitel hatten wir uns mit Primelementen und irreduziblen Elementen eines Ringes beschäftigt und dabei den Blick vor allem auf Hauptideale gelegt. Für die wichtige Klasse der Euklidischen Ringe und allgemeiner für Hauptidealringe konnten wir nach diesen Überlegungen dann auch Faktorialität zeigen. Entscheidend dabei war die Teilerkettenbedingung für *Hauptideale* sowie die Äquivalenz von *prim* und *irreduzibel* in Hauptidealringen.

Danach hatten wir explizite Restklassenkonstruktionen ($\mathbb{Z}/m\mathbb{Z}$, $K[t]/\langle h\rangle$) kennengelernt, bei denen die Äquivalenzrelation durch Hauptideale gegeben ist, und waren schließlich zu den Isomorphiesätzen gekommen, die Bilder von Abbildungen und Faktorringe verbinden. Allerdings ist bei weitem nicht jeder Ring ein Hauptidealring und daher können wir nicht erwarten, dass Kerne von Ringhomomorphismen sich immer als Hauptideale erweisen werden. Jenseits der Hauptideale würden wir uns daher eine Verallgemeinerung der Begriffe *prim* und *irreduzibel* wünschen, um Aussagen über Eigenschaften von Ringen der Form R/I treffen zu können.

Definition 4.6.1 *Sei R ein kommutativer Ring*[1]*. Ein echtes Ideal $\mathfrak{m} \trianglelefteq R$ heißt* **maximales Ideal**, *falls*

$$\forall I \trianglelefteq R \text{ mit } \mathfrak{m} \subseteq I \subseteq R: \quad (I = \mathfrak{m} \text{ oder } I = R).$$

Ein maximales Ideal ist als ein echtes Ideal, das maximal ist unter der Inklusion von Idealen.

[1] wie immer mit 1.

Lemma 4.6.2 *Sei R ein Hauptidealring und sei $c \in R \setminus (\{0\} \cup R^*)$. c ist irreduzibel genau dann, wenn $\langle c \rangle$ maximal ist.*

Beweis: "$\Longrightarrow$" Sei $I \trianglelefteq R$ ein Ideal mit $\langle c \rangle \subseteq I \subseteq R$. Da R ein Hauptidealring ist, existiert ein $d \in R$ mit $I = \langle d \rangle$. Wegen $\langle c \rangle \subseteq \langle d \rangle$ gilt aber $d \mid c$. Aus der Irreduzibilität von c folgt dann, dass $d \sim c$ oder $d \in R^*$. Im ersteren Fall ist $\langle d \rangle = \langle c \rangle$, im letzteren ist $\langle d \rangle = R$, womit die Maximalität von $\langle c \rangle$ gezeigt ist.
"$\Longleftarrow$" Sei umgekehrt $\langle c \rangle$ maximales Ideal in R und sei $d \in R$ ein Teiler von c. Dann gilt $\langle c \rangle \subseteq \langle d \rangle \subseteq R$, weswegen nach Maximalität gilt $\langle c \rangle = \langle d \rangle$, d.h. $c \sim d$, oder $\langle d \rangle = R$, d.h. $d \in R^*$. Damit ist die Irreduzibilität von c beweisen.

□

Bemerkung 4.6.3 *Schwächen wir die Bedingung 'Hauptidealring' ab zu 'Integritätsring', so läßt sich noch immer eine etwas schwächere Aussage treffen: $c \in R$ ist irreduzibel genau dann, wenn $\langle c \rangle$ maximal unter Inklusion von Hauptidealen ist. Das Vorgehen des Beweises bleibt dasselbe, die leichte Abschwächung der Aussage trägt lediglich solchen Situationen Rechnung, in denen $c \in R$ irreduzibel ist, es aber ein $d \in R$ gibt mit $\langle c \rangle \subsetneq \langle c, d \rangle \subsetneq R$.*

Definition 4.6.4 *Sei R ein kommutativer Ring. Ein echtes Ideal $\mathfrak{p} \trianglelefteq R$ heißt ein Primideal in R, falls*

$$\forall a, b \in R : (a \cdot b \in \mathfrak{p} \Longrightarrow (a \in \mathfrak{p} \text{ oder } b \in \mathfrak{p})).$$

Lemma 4.6.5 *Sei R ein Integritätsring und sei $p \in R \setminus (\{0\} \cup R^*)$. p ist prim genau dann, wenn $\langle p \rangle$ ein Primideal ist.*

Der Beweis dieses Lemmas folgt durch direkte Verwendung der Definitionen Primelement und Primideal – völlig analog dazu, wie wir es im vorigen Lemma mit den Definitionen irreduzibel und maximal gesehen haben. Der Beweis bleibt damit als Übungsaufgabe.

Korollar 4.6.6 *(zu den Definitionen) In einem kommutativen Ring ist jedes maximale Ideal prim.*

Beweis: Sei $\mathfrak{m} \trianglelefteq R$ ein maximales Ideal in einem kommutativen Ring R und seien $a, b \in R$ mit $a \cdot b \in \mathfrak{m}$. Betrachte das Ideal $\mathfrak{m} + \langle b \rangle$. Für dieses gilt

$$\mathfrak{m} \subseteq \mathfrak{m} + \langle b \rangle \subseteq R$$

und daher sind wegen der Maximalität von $\mathfrak{m}$ nur $\mathfrak{m} = \mathfrak{m} + \langle b \rangle$, d.h. $b \in \mathfrak{m}$, oder $\mathfrak{m} + \langle b \rangle = R$, d.h. $[b]_\mathfrak{m} \in (R/\mathfrak{m})^*$, möglich. Im letzteren Fall existiert aber eine Inverse $[c]_\mathfrak{m}$ zu $[b]_\mathfrak{m}$, d.h. es gibt ein $x \in \mathfrak{m}$ mit $x + b \cdot c = 1$. Aber dann ist

$$a = a \cdot (x + b \cdot c) = a \cdot \underbrace{x}_{\in \mathfrak{m}} + \underbrace{(a \cdot b)}_{\in \mathfrak{m}} \cdot c \in \mathfrak{m}.$$

Daher ist $\mathfrak{m}$ Primideal.

□

Korollar 4.6.7 *(zu den Definitionen und Satz 3.1.6) In einem Hauptidealring ist jedes Primideal, das nicht das Nullideal ist, maximal.*

Beweis: In einem Hauptidealring stimmen die Begriffe *irreduzibel* und *prim* überein. Die Lemmata 4.6.2 und 4.6.5 übertragen das gerade auf maximale Ideale und Primideale.

□

Satz 4.6.8 *Sei R kommutativer Ring und sei $I \trianglelefteq R$ ein echtes Ideal. Dann gilt:*

$$I \text{ ist Primideal} \iff R/I \text{ ist Integritätsring.}$$

Beweis: Vorab bemerken wir, dass $a \in I$ äquivalent zu $[a]_I = [0]_I$ ist nach der Definition von R/I. Die Bedingung I ist Primideal bedeutet gerade

$$\forall a, b \in R \text{ mit } a \cdot b \in I : (a \in I \text{ oder } b \in I).$$

Mit der gerade beobachteten Äquivalenz ist das dasselbe wie

$$\forall [a]_I, [b]_I \in R/I \text{ mit } [a \cdot b]_I = [0]_I : ([a]_I = [0]_I \text{ oder } [b]_I = [0]_I).$$

Das ist aber gerade die Aussage der Nullteilerfreiheit in R/I. Da R und damit R/I nach Voraussetzung kommutativ sind, ist das auch die Integritätsringeigenschaft von R/I.

□

Satz 4.6.9 *Sei R kommutativer Ring und sei $I \trianglelefteq R$ ein echtes Ideal. Dann gilt:*

$$I \text{ maximales Ideal} \iff R/I \text{ Körper.}$$

Beweis: Bezeichne mit $\pi : R \longrightarrow R/I$ den kanonischen Restklassenepimorphismus.
Ist I maximal, so gilt für jedes Element $a \in R \setminus I$: $I + \langle a \rangle = R$. Daher gilt auch

$$\langle \pi(a) \rangle = [0]_I + \langle \pi(a) \rangle = R/I.$$

Wegen der Surjektivität von π kann es in R/I also nur zwei Ideale geben, den ganzen Ring und das Nullideal. Damit ist R/I nach Lemma 2.6.7 ein Körper.
Ist andererseits $J \trianglelefteq R$ ein echtes Ideal mit $I \subsetneq J$, so ist $\langle [0]_I \rangle \subsetneq \pi(J) \subsetneq R/I$ und R/I damit nach Lemma 2.6.7 kein Körper.

□

Bemerkung 4.6.10 *Mit Hilfe der letzten beiden Sätze haben wir jetzt einen weiteren, viel einfacheren Beweis für Korollar 4.6.6: Jeder Körper ist Integritätsring, damit muss jedes maximale Ideal prim sein.*

Zum Abschluß der theoretischen Betrachtungen dieses Abschnitts fassen wir nochmals die verschiedenen Aussagen in neuer Weise zusammen:

Satz 4.6.11 *In einem Hauptidealring R sind für ein $a \in R \setminus \{0\}$ äquivalent:*

a) a ist Primelement

b) $R/\langle a \rangle$ ist Integritätsring

c) $R/\langle a \rangle$ ist Körper

Beweis: Dies ist die Zusammenstellung für den Fall eines Hauptidealrings von 4.6.7, 4.6.8 und 4.6.9.

□

Satz 4.6.12 *Sei R ein kommutativer Ring[2]. Dann sind äquivalent:*

a) R ist Körper

b) R hat keine echten Ideale

[2] mit $1 \neq 0$ wie üblich

c) $\forall I \trianglelefteq R$ *mit* $\langle 0_R\rangle \subseteq I \subseteq R : (I = \langle 0\rangle$ *oder* $I = R)$
(Wäre $\langle 0\rangle$ *echtes Ideal, so würde man sagen, dass* $\langle 0\rangle$ *maximales Ideal von* R *ist.)*

Beweis: Das ist die Zusammenstellung von 2.6.7 und 4.6.9 mit Blick auf Ideale in R.

□

Damit dieser Stoff nicht so trocken bleibt, wie er auf den ersten Blick aussieht, wenden wir dies dann auch wieder auf die früher definierten Restklassenringe an:

Anwendung 4.6.13 *Aus Satz 4.6.11 sehen wir sofort:*

$$\mathbb{Z}/m\mathbb{Z} \text{ Körper} \iff m \text{ Primzahl}$$

sowie für einen Körper K*:*

$$K[t]/\langle h\rangle \text{ Körper} \iff h \text{ irreduzibles Polynom}$$

Anwendung 4.6.14 *Betrachten wir* $I = \langle 3, t^2+1\rangle \subset \mathbb{Z}[t]$*. Dies ist offensichtlich kein Hauptideal. Untersuchen wir* $\mathbb{Z}[t]/I$ *nun, indem wir zuerst den Restklassenring von* $\mathbb{Z}[t]$ *bzgl.* $\langle 3\rangle$ *bilden. Dieses Vorgehen ist abgedeckt durch den zweiten Isomorphiesatz, der sicherstellt, dass*

$$(\mathbb{Z}[t]/\langle 3\rangle)/(\langle 3, t^2+1\rangle/\langle 3\rangle) = \mathbb{Z}[t]/\langle 3, t^2+1\rangle.$$

Mit einem kurzen Blick auf die Definition eines Polynomrings als Folge von Elementen des Grundrings ist direkt klar, dass die Restklassenbildung sich rein in den Koeffizienten abspielt und damit $\mathbb{Z}[t]/\langle 3\rangle = (\mathbb{Z}/\langle 3\rangle)[t]$*. Wir sehen also einen Polynomring über dem Körper* $\mathbb{Z}/\langle 3\rangle$ *vor uns.* t^2+1 *besitzt keine Nullstellen im Körper* $\mathbb{Z}/\langle 3\rangle$ *und damit ist* $(\mathbb{Z}/\langle 3\rangle)[t]/\langle t^2+1\rangle$ *ein Körper. Daher ist* I *maximales Ideal.*
Der Körper $(\mathbb{Z}/\langle 3\rangle)[t]/\langle t^2+1\rangle$ *hat übrigens genau* 3^2 *Elemente. Überlegen Sie welche und warum.*

Bemerkung 4.6.15 *Sei* R *ein kommutativer Ring und sei* $g \in R\backslash(\{0\}\cup R^*)$*. Dann gilt für alle* $a, c, x \in R$*:*

$$[a]_g \cdot [x]_g = [c]_g \iff \exists y \in R : ax + gy = c.$$

Bemerkung 4.6.16 *Ist* R *ein euklidischer Ring, so folgt aus der vorigen Bemerkung für alle* $a \in R \setminus \{0\}$*:*

$$[a]_g \in (R/\langle g\rangle)^* \iff 1 \text{ ist ein größter gemeinsamer Teiler von } a \text{ und } g.$$

4.7 Chinesischer Restsatz

Bisher haben wir uns vor allem mit dem Fall von Restklassenringen nach Primidealen und maximalen Idealen befasst. Diese haben als Integritätsringe bzw. Körper natürlich sehr schöne Eigeneschaften, in ihnen läßt sich vor allem relativ problemlos rechnen. Aber dadurch sind bei weitem nicht alle Fälle abgedeckt. Daher wenden wir uns in diesem Abschnitt dem Chinesischen Restsatz zu, der es z.B. erlaubt, im Falle des Restklassenrings von $\mathbb{Z}$ bzgl. einer zusammengesetzten Zahl mit r paarweise verschiedenene Primfaktoren stattdessen in r verschiedenen Integritätsringen zu rechnen.

Wir werden den Chinesischen Restsatz zuerst in einer sehr allgemeinen Form beweisen, dann aber auch die wichtigen Spezialfälle in $\mathbb{Z}$ und $K[t]$ daraus folgern. Wie auch mit vielen anderen Begriffen, die wir für die ganzen Zahlen schon lange kennen und in den vergangenen Kapiteln auf größere Klassen von Ringen verallgemeinert haben, müssen wir auch hier erst einen Begriff neu definieren: Teilerfremdheit von Idealen.

Erinnerung 4.7.1 *Sei R ein faktorieller Ring. Elemente $a_1, \ldots, a_n \in R$ heißen teilerfremd (oder coprim), falls ihre einzigen gemeinsamen Teiler Einheiten in R sind, d.h. in der Sprache von Abschnitt 4.4 bei gegebenem Repräsentantensystem $\mathcal{P}$ von R bzgl. Assoziiertheit, dass*

$$\min\{v_p(a_1), \ldots, v_p(a_n)\} = 0 \quad \forall p \in \mathcal{P} \setminus [1_R].$$

Für die folgende Erinnerung müssen wir die betrachteten Ringe etwas weiter einschränken, da sie nicht nur von der Existenz eines größten gemeinsamen Teilers abhängt, sondern von der Bézout-Identität, die nur in Hauptidealringen gilt.

Erinnerung 4.7.2 *Sei R Hauptidealring. Sind $a, b \in R$ teilerfremd, so gilt:*

$$\langle a \rangle + \langle b \rangle = R.$$

In der Tat ist die letztere Eigenschaft für eine Verallgemeinerung des Begriffs der Teilerfremdheit auf Ideale besser geeignet, als die erstere, da sie bereits von Idealen handelt.

Definition 4.7.3 *Sei R ein Integritätsring. Zwei Ideale $I, J \trianglelefteq R$ heißen* **teilerfremd** *(oder* **coprim** *oder* **relativ prim***), falls:*

$$I + J = R.$$

Ideale $I_1, \ldots, I_n \trianglelefteq R$ heißen **paarweise teilerfremd**, *falls:*

$$I_i + I_j = R \ \forall 1 \leq i < j \leq n.$$

Betrachten wir nun ein Beispiel für das zentrale Problem dieses Kapitels und dessen Lösung:

Beispiel 4.7.4 *In seinem Handbuch zur Arithmetik schrieb Sun Zi vor mehr als 2000 Jahren bereits über ein Problem, das wir heute als eine Aufgabe in einem nicht nullteilerfreien Restklassenring auffassen würden:*

> *Wir haben eine gewisse Zahl von Dingen, wissen jedoch nicht genau wieviele. Wenn wir sie je drei zählen, so verbleiben zwei. Wenn wir sie je fünf zählen, so verbleiben drei. Wenn wir sie je sieben zählen, sind noch zwei übrig. Wieviele Dinge sind es?*

Zusätzlich möchten wir noch voraussetzen, dass die Zahl zwischen 100 und 200 liegt.
Im heutigen Formalismus der Algebra lautet dann die Aufgabe:
Finde eine Zahl $\tilde{x} \in \mathbb{N}_0$ mit $100 \leq \tilde{x} \leq 200$, so dass gilt:

$$\begin{aligned} \tilde{x} &\equiv 2 \bmod 3 \\ \tilde{x} &\equiv 3 \bmod 5 \\ \tilde{x} &\equiv 2 \bmod 7 \end{aligned}$$

Um diese zu lösen, bilden wir zuerst die folgenden Zahlen:

$$m_1 = 3, \quad m_2 = 5, \quad m_3 = 7, \quad m := 3 \cdot 5 \cdot 7 = 105.$$

Wichtig dabei ist, dass m kongruent Null modulo jeder der drei Zahlen m_1, m_2, m_3 ist. Nun bilden wir noch

$$N_1 = \frac{m}{m_1} = 35 \quad N_2 = \frac{m}{m_2} = 21 \quad N_3 = \frac{m}{m_3} = 15$$

Damit ist jedes der N_i teilerfremd zu dem entsprechenden m_i und kongruent Null zu den beiden anderen m_j. Insbesondere besitzt N_i damit ein multiplikatives Inverses y_i modulo m_i:

$$\begin{aligned} [N_1]_{m_1} = [35]_3 = [2]_3 &\implies [N_1]_3 \cdot [y_1]_3 = [2]_3 \cdot [2]_3 = [1]_3 \\ [N_2]_{m_2} = [21]_5 = [1]_5 &\implies [N_2]_5 \cdot [y_2]_5 = [1]_5 \cdot [1]_5 = [1]_5 \\ [N_3]_{m_3} = [15]_7 = [1]_7 &\implies [N_3]_7 \cdot [y_3]_7 = [1]_7 \cdot [1]_7 = [1]_7 \end{aligned}$$

Betrachten wir nun $x_0 = 2 \cdot N_1 \cdot y_1 + 3 \cdot N_2 \cdot y_2 + 2 \cdot N_3 \cdot y_3 = 233$*, so ergeben sich die gewünschten Kongruenzen (Nachrechnen!). Wir haben damit eine Lösung des Kongruenzsystems gefunden, aber es ist nicht die einzige und es ist nicht die gesuchte! Wir können aber zu* x_0 *genau beliebige Vielfache von* $m = 105$ *hinzuaddieren, ohne die drei Kongruenzen zu verändern. Damit ist die Lösungsmenge des Kongruenzsystems:*

$$\{233 + 105k \mid k \in \mathbb{Z}\}.$$

Für das konkrete Problem erhalten wir die Lösung $\tilde{x} = 233 - 105 = 128$*.*

Das obige Beispiel ist in einer Form aufgeschrieben, die bereits die Grundideen des Beweises des allgemeinen Satzes vorwegnimmt und daher beim Nacharbeiten als Leitfaden durch den Beweis verwendet werden kann. Doch es ist nicht absolut offensichtlich, die einzelnen Schritte zuzuordnen. Wer es nicht direkt hinbekommt, findet im Vergleich von Korollar 4.7.10 und Satz 4.7.5 Hinweise darauf, wie die einzelnen Fakten und Konstruktionen zusammenspielen.

Satz 4.7.5 *(Chinesischer Restsatz, allgemeine Formulierung) Sei* R *ein Integritätsring und seien* $I_1, \ldots, I_n$ *paarweise teilerfremde Ideale von* R*. Für jede gegebene Wahl von* $r_1, \ldots, r_n \in R$ *existiert ein* $b \in R$*, das die simultanen Kongruenzen*

$$\begin{aligned} b &\equiv r_1 \bmod I_1 \\ &\vdots \\ b &\equiv r_n \bmod I_n \end{aligned}$$

erfüllt. Die Lösung b *ist eindeutig modulo* $I_1 \cdot \cdots \cdot I_n = I_1 \cap \cdots \cap I_n$*.*

Da der Beweis etwas länglich und unübersichtlich werden kann, wenn man ihn in einem Stück ausführt, betrachten wir vorher mehrere Lemmata:

Lemma 4.7.6 *Sei* R *ein Integritätsring und seien* I_1, I_2 *teilerfremde Ideale in* R*. Dann existiert für jede Wahl von* $r_1, r_2 \in R$ *ein* $b \in R$*, das die simultanen Kongruenzen*

$$\begin{aligned} b &\equiv r_1 \bmod I_1 \\ b &\equiv r_2 \bmod I_2 \end{aligned}$$

erfüllt. Die Lösung b *ist eindeutig modulo* $I_1 \cdot I_2 = I_1 \cap I_2$*.*

Beweis: Da I_1 und I_2 coprim sind und damit $I_1 + I_2 = R$ gilt, existieren $x_1 \in I_1$ und $x_2 \in I_2$ mit $x_1 + x_2 = 1$. Insbesondere gilt dann

$$\begin{aligned} [x_2]_{I_1} &= [x_1 + x_2]_{I_1} = [1]_{I_1} \text{ und} \\ [x_1]_{I_2} &= [x_1 + x_2]_{I_2} = [1]_{I_2}. \end{aligned}$$

Betrachten wir nun

$$b = x_1 \cdot r_1 + x_2 \cdot r_2 \in R,$$

so gilt

$$\begin{aligned} [b]_{I_1} &= [r_2 x_2]_{I_1} = [r_2]_{I_1} \cdot [x_2]_{I_1} = [r_2]_{I_1} \\ [b]_{I_2} &= [r_1 x_1]_{I_2} = [r_1]_{I_2} \cdot [x_1]_{I_2} = [r_1]_{I_2}. \end{aligned}$$

Damit erfüllt b die Bedingungen des Satzes.
Für die Eindeutigkeit seien nun $b, c \in R$ zwei Lösungen des Kongruenzproblems. Dann gilt $[b]_{I_1} = [r_1]_{I_1} = [c]_{I_1}$ und $[b]_{I_2} = [r_2]_{I_2} = [c]_{I_2}$, weshalb $b - c \in I_1 \cap I_2$ gelten muss. Umgekehrt ändert das Hinzuaddieren eines Elements aus $I_1 \cap I_2$ die Restklassen modulo I_1 und I_2 nicht, womit gezeigt ist, dass die Lösungsmenge des Kongruenzsystems bei einer bekannten Lösung $b \in R$ genau die Menge

$$\{b + h \mid h \in I_1 \cap I_2\}$$

ist.

□

Lemma 4.7.7 *Sei R ein Integritätsring, seien $I_1, \ldots, I_n$ paarweise teilerfremde Ideale von R und sei $1 \leq i \leq n$ ein fester Index. Dann gilt*

$$I_i + \bigcap_{\substack{1 \leq j \leq n \\ j \neq i}} I_j = R.$$

Beweis: Da die Ideale paarweise teilerfremd sind, wissen wir, dass es zu jedem Paar von Indizes (i, j) mit $j \neq i$ Elemente $c_j \in I_i$ und $d_j \in I_j$ gibt mit $c_j + d_j = 1$. Wir rechnen:

$$1 = \prod_{\substack{1 \leq j \leq n \\ j \neq i}} (c_j + d_j) = f(\underline{c}, \underline{d}) + \prod_{\substack{1 \leq j \leq n \\ j \neq i}} d_j,$$

wobei im Ausdruck f jeder Summand durch mindestens ein c_j teilbar ist, weswegen $f(\underline{c}, \underline{d}) \in I_i$. Andererseits gilt offensichtlich

$$\prod_{\substack{1 \leq j \leq n \\ j \neq i}} d_j \in \bigcap_{\substack{1 \leq j \leq n \\ j \neq i}} I_j.$$

Damit sind f und das Produkt über die d_j die beiden gesuchten Summanden.

□

Mit Hilfe dieser beiden Lemmata ist der Beweis des Satzes dann ganz übersichtlich:

Beweis: (4.7.5)
Nach Lemma 4.7.6 ist die Aussage für $n = 2$ Ideale bewiesen, was wir als Induktionsanfang einer Induktion nach n verwenden. Nehmen wir als Induktionsvoraussetzung an, dass die Behauptung für $n - 1$ Ideale gilt. Im Induktionsschritt schließen wir nun von $n - 1$ auf n Ideale:
Sind $I_1, \ldots, I_n$ paarweise teilerfremde Ideale in R, so sind nach Lemma 4.7.7 auch $J = \bigcap_{1 \leq i \leq n-1} I_i$ und I_n teilerfremde Ideale. Für die simultane Kongruenz bzgl. der $n - 1$ Ideale $I_1, \ldots, I_{n-1}$ existiert ein b_1, das diese löst und modulo J eindeutig ist. Das liefert uns ein neues System simultaner Kongruenzen:

$$\begin{aligned} [b]_{I_n} &= [r_n]_{I_n} \\ [b]_J &= [b_1]_J, \end{aligned}$$

welches wieder nach Induktionsanfang eine modulo $J \cdot I_n$ eindeutige Lösung b besitzt.

□

Bemerkung 4.7.8 *Seien $R_1, \ldots, R_n$ Ringe. Dann bezeichnet $R_1 \times \cdots \times R_n$ die Menge aller n-Tupel aus Einträgen aus R_1 bis R_n. Auf dieser Menge lassen sich durch komponentenweise Addition und Multiplikation zwei Verknüpfungen definieren, bzgl. derer diese Menge wieder ein Ring ist. Die Überprüfung der Ringaxiome ist eine leicht längliche, explizite Rechnung, die keine Schwierigkeiten bietet und deshalb hier entfällt. Das Einselement des neuen Ringes ist $(1_{R_1}, \ldots, 1_{R_n})$.*

Korollar 4.7.9 *Sei R Integritätsring und seien $I_1, \ldots, I_n$ paarweise teilerfremde Ideale in R. Dann ist*

$$R \Big/ \left(\prod_{i=1}^{n} I_i \right) \cong (R/I_1) \times \cdots \times (R/I_n)$$

ein Ringisomorphismus, der $[r]_{(\prod_{i=1}^{n} I_i)}$ auf das Tupel der $[r]_{I_i}$ abbildet.

Beweis: Da jedes einzelne R/I_j ein Ring ist, ist auch die Menge auf der rechten Seite bzgl. der komponentenweisen Addition und Multiplikation ein Ring. Die Abbildung

$$\begin{array}{rcl} \varphi : R & \longrightarrow & (R/I_1) \times \cdots \times (R/I_n) \\ b & \longmapsto & ([b]_{I_1}, \ldots, [b]_{I_n}) \end{array}$$

ist komponentenweise aus Restklassenhomomorphismen zusammengesetzt, die (wie wir bereits wissen) jeweils Ringepimorphismen sind. Da die Verknüpfungen auf der rechten Seite ebenfalls komponenteweise definiert sind, ist auch φ ein Ringhomomorphismus (Nachrechnen!). Nach Satz 4.7.5 besitzt jedes System von simultanen Kongruenzen modulo I_1 bis I_n eine Lösung in R, so dass φ surjektiv ist. Ebenfalls nach 4.7.5 ist das Urbild der Null unter φ gerade das Produkt der Ideale $I_1 \cdots I_n$. Damit folgt die Aussage des Korollars aus dem Homomorphiesatz.

□

Den allgemeinen Satz können wir auch spezieller für Hauptidealringe oder noch konkreter für $\mathbb{Z}$ oder den Polynomring $K[t]$ über einem Körper K formulieren. Da es sich dabei lediglich um die direkte Anwendung des Satzes in einer konkretisierten Situation handelt, müssen wir diese Aussagen nicht beweisen.

Korollar 4.7.10 *(Chinesischer Restsatz für Hauptidealringe) Sei R ein Hauptidealring und seien $m_1, \ldots, m_n \in R$ paarweise teilerfremd. Zu gegebenen $r_1, \ldots, r_n \in R$ existiert dann ein $b \in R$, das das folgende System von simultanen Kongruenzen löst:*

$$[X]_{m_i} = [r_i]_{m_i} \quad \forall 1 \leq i \leq n.$$

Die Lösung ist modulo $m := m_1 \cdot \cdots \cdot m_n$ eindeutig und es gilt:

$$R/\langle m \rangle \cong (R/\langle m_1 \rangle) \times \cdots \times (R/\langle m_n \rangle)\,.$$

Korollar 4.7.11 *(Chinesischer Restsatz für Hauptidealringe, Version 2) Sei R ein Hauptidealring und sei $a \in R \setminus (\{0\} \cup R^*)$ mit Primfaktorzerlegung*

$$a = \varepsilon(a) \prod_{i=1}^{n} p_i^{e_i},$$

wobei $\varepsilon(a) \in R^*$ und $e_1, \ldots, e_n \in \mathbb{N}$ sowie $p_1, \ldots, p_n \in R$ paarweise nicht assoziierte Primelemente in R sind. Dann gilt

$$R/\langle a \rangle \cong (R/\langle p_1^{e_1} \rangle) \times \cdots \times (R/\langle p_n^{e_n} \rangle).$$

Vergleichen Sie die beiden vorstehenden Korollare und bringen Sie die beiden Aussagen in Einklang. Wir spielen hier gerade mit verschiedenen Anwendungen desselben Satzes auf verschiedene Situationen und deren Formulierung. Unabhängig vom hier gewählten Kontext, in dem wir das gerade üben, ist die Fähigkeit, allgemeine Sätze auf konkrete Kontexte anwenden zu können, ohne sie jedesmal in einer neuen Situation wieder beweisen zu müssen, ein wichtiges Charakteristikum der Mathematik. Man begibt sich in einen recht allgemeinen Kontext (mit genau den Voraussetzungen, die man wirklich braucht), formuliert und beweist die gewünschte Aussage und wendet sie dann später in ganz verschiedenen Situationen an.

Bemerkung 4.7.12 *(Wie 'basteln' wir b konkret?)*
In der Situation des Satzes 4.7.10 wissen wir, dass die paarweise teilerfremden Ideale von der Form $I_i = \langle m_i \rangle$ sind. Wir definieren:

$$\begin{aligned} N &:= m_1 \cdots m_n \\ N_i &:= \prod_{\substack{1 \le j \le n \\ j \neq i}} m_j \end{aligned}$$

Dann gilt $\prod_{i=1}^{n} I_i = \langle N \rangle$ und $\prod_{\substack{1 \le j \le n \\ j \neq i}} I_j = \langle N_i \rangle$. Da m_i und N_i (für ein festes i) nach Konstruktion teilerfremd sind, ist N_i nach dem Satz von Bézout invertierbar in $R/\langle m_i \rangle$. Dieses Inverse nennen wir y_i. Damit kann man leicht explizit nachrechnen, dass

$$b = \sum_{i=1}^{n} r_i N_i y_i$$

das gewünschte System von simultanen Kongruenzen erfüllt.

Die folgende weitere Konkretisierung des Rings mit Formulierung der entsprechenden Aussage trägt den Namen 'Fundamentalsatz', ist aber mit unseren bisher bewiesenen Techniken nichts als ein direktes Korollar. Den Namen verdient der Satz wegen seiner großen Bedeutung in Theorie (als Strukturssatz) und Praxis. Eine recht naheliegende, aber auch wichtige Anwendung das sogenannte 'modulare' Rechnen in der Computeralgebra: In vielen Algorithmen mit Berechnungen über den ganzen Zahlen wachsen die betrachteten Zahlen zwischenzeitlich sehr schnell an, so dass die Rechnungen allein durch die großen Zahlen schon speicherintensiv und damit langsam werden können. Hat man vorab eine Abschätzung, wie groß die Zahlen, z.B. Koeffizienten eines polynomialen Ergebnisses, werden können, ist es statt der Rechnung über $\mathbb{Z}$ möglich über ausreichend vielen, verschiedenen Körpern $\mathbb{Z}/p\mathbb{Z}$ zu rechnen und das Ergebnis am Ende mit dem Chinesischen Restsatz zu bestimmen.

Satz 4.7.13 *(Fundamentalsatz für $\mathbb{Z}/m\mathbb{Z}$) Für alle $m \in \mathbb{N}$ mit teilerfremder Zerlegung $m = \prod_{i=1}^{n} m_i$ gilt*

$$\mathbb{Z}/m\mathbb{Z} \cong (\mathbb{Z}/m_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/m_n\mathbb{Z})\,.$$

Die Formulierung des Chinesischen Restsatzes für univariate Polynomringe über einem Körper werden Sie als Übungsaufgabe vorfinden.

4.8 Quotientenkörper und Lokalisierung

Viele der altbekannten Eigenschaften von $\mathbb{Z}$ haben wir schon in allgemeinen Kontext stellen können. Noch nicht betrachtet haben wir die Konstruktion der rationalen Zahlen $\mathbb{Q}$ aus den ganzen Zahlen $\mathbb{Z}$. Dies holen wir in dem folgenden recht kurzen Abschnitt nach. Für die 2-Fächer Bachelor ist lediglich die Konstruktion des Quotientenkörpers relevant, der allgemeinere Kontext der Lokalisierung ist nur für die Fachmathematiker verpflichtend.

Bemerkung 4.8.1 *Sei R ein Integritätsring und sei $S = R \times (R \setminus \{0\})$ die Menge aller Paare von Elementen aus R, bei denen das zweite nicht Null ist. Dann können wir auf S eine kommutative Ringstruktur definieren mittels der Verknüpfungen*

$$\begin{aligned} + : S \times S &\longrightarrow S \\ ((a,b),(c,d)) &\longmapsto (ad+bc, bd) \\ \cdot : S \times S &\longrightarrow S \\ ((a,b),(c,d)) &\longmapsto (ac, bd). \end{aligned}$$

Die Tatsache, dass es sich bei $(S, +, \cdot)$ tatsächlich um einen Ring handelt, läßt sich ohne Probleme direkt nachrechnen.

Satz 4.8.2 *Sei R ein Integritätsring. Dann ist durch auf der Menge $S = R \times (R \setminus \{0\})$ eine Äquivalenzrelation definiert durch*

$$(a, b) \sim (c, d) :\Longleftrightarrow ad - bc = 0.$$

$S/\sim$ ist ein Körper, der R enthält, der **Quotientenkörper** *von R, kurz $Quot(R)$.*

Beweis: $\sim$ ist offensichtlich reflexiv, da $ab - ab = 0$, und symmetrisch, da $bc - ad = -(ad - bc) = 0$. Für die Transitivität betrachten wir drei Paare $(a, b), (c, d), (e, f) \in S$, so dass $ad - bc = 0$ und $cf - de = 0$. Ist $c = 0$, so ist nach diesen Gleichungen, nach der Nullteilerfreiheit von R und nach der Voraussetzung $d \in R \setminus \{0\}$ auch $a = e = 0$, weshalb die gewünschte Gleichung $af - be = 0$ automatisch erfüllt ist. Bleibt der Fall $c \neq 0$ zu betrachten. Hierbei rechnen wir:

$$0 = e \cdot (ad - bc) + a \cdot (cf - de) = ade - bce + acf - ade = acf - bce.$$

Da aber R nullteilerfrei ist und da $c \neq 0$, muss damit gelten, dass $af - be = 0$, was uns die Transitivität von $\sim$ liefert. Damit ist $\sim$ eine Äquivalenzrelation auf S. $S/\sim$ ist wieder ein Ring (Nachrechnen!).
Zum Beweis, dass $S/\sim$ ein Körper ist, sei $0_{S/\sim} \neq s \in S/\sim$ beliebig und sei $(a, b) \in S$ ein Repräsentant von s. Dann ist insbesondere $a \neq 0$ und wir können das Paar $(b, a) \in S$ betrachten. Es gilt

$$(a, b) \cdot (b, a) = (ab, ab) \sim (1, 1),$$

d.h.

$$[(a, b)]_\sim \cdot [(b, a)]_\sim = 1_{S/\sim},$$

womit ein Inverses zu s bestimmt ist. Daher ist $S/\sim$ ein Körper. Wir betrachten jetzt die Komposition von Ringhomomorphismen:

$$\begin{array}{ccc} R & \hookrightarrow & S \longrightarrow S/\sim \\ r & \longmapsto & (r, 1) \longmapsto [(r, 1)]_\sim, \end{array}$$

wobei die erste Abbildung injektiv ist. Damit wir tatsächlich $R \subset S/\sim$ erhalten, muss auch die Verkettung der beiden Abbildungen injektiv sein.

Seien dazu $r_1 \neq r_2 \in R$, dann gilt $(r_1, 1) \neq (r_2, 1)$ und auch $[(r_1, 1)]_\sim \neq [(r_2, 1)]_\sim$ wegen $r_1 \cdot 1 - r_2 \cdot 1 = r_1 - r_2 \neq 0$. Daher ist die Komposition der beiden obigen Abbildungen injektiv und alle Behauptungen des Satzes sind gezeigt.

□

Erkennen Sie die Konstruktion? Die Addition und die Multiplikation sind gerade so definiert, wie es die Addition und Multiplikation von Brüchen, dargestellt als Paar (Zähler, Nenner), erfordert. Nehmen Sie als R die ganzen Zahlen $\mathbb{Z}$, dann ist die Äquivalenzrelation die Gleichheit nach Kürzen bzw. Erweitern und $S/\sim$ ist dann der Körper der rationalen Zahlen $\mathbb{Q}$.

Die obige Konstruktion ist ein Spezialfall einer allgemeineren Konstruktion der Lokalisierung. Diese werden wir in der kommutativen Algebra ausführlich besprechen. Hier geben wir lediglich die Definition an und nennen einige wichtige Eigenschaften im Vorgriff auf diese Veranstaltung.

Definition 4.8.3 *Eine Teilmenge $S \neq \emptyset$ eines kommutativen Ringes R heißt* **multiplikativ abgeschlossen**, *falls $1 \in S$ und für $a, b \in S$ auch $a \cdot b \in S$. Auf $R \times S$ definieren wir eine Relation durch*

$$(r, a) \sim (s, b) :\Longleftrightarrow \quad \exists v \in S : v(rb - sa) = 0$$

Bemerkung 4.8.4 *Hier könnte man noch fordern, dass $0 \notin S$. Damit würde man einen pathologischen Fall ausschliessen, denn wenn $0 \in S$, dann fallen alle Elemente beim Bilden von $S^{-1}R$ mit der Null zusammen und wir erhalten einen Ring mit nur einem Element. Ob man dies explizit ausschließen möchte oder nicht, ist Geschmacksache.*
Ist R nullteilerfrei oder enthält S keine Nullteiler von R, so ist die Bedingung $v(rb - sa) = 0$ gleichbedeutend mit $rb - sa = 0$. Einzig im Falle eines Nullteilers $v \in S$, kann es vorkommen, dass für zwei Paare (r, a) und (s, b) gilt $rb - sa \neq 0$, während $v(rb - sa) = 0$.

Satz 4.8.5 *Die Relation aus Definition 4.8.3 ist eine Äquivalenzrelation.*

Definition 4.8.6 *Sei R kommutativer Ring, $S \subseteq R$ multiplikativ abgeschlossene Teilmenge und $\sim$ die in 4.8.3 definierte Äquivalenzrelation. Für $(r, a) \in R \times S$ bezeichne die zugehörige Klasse von (r, a) durch*

$$\frac{r}{a} := [(r, a)]_\sim = \{(s, b) \in R \times S \mid (r, a) \sim (s, b)\}.$$

Die **Lokalisierung** *von R nach S ist dann die Menge der Äquivalenzklassen bzgl. $\sim$, kurz*

$$S^{-1}R := \{\frac{r}{a} \mid r \in R, a \in S\}.$$

Bemerkung 4.8.7 *Sei R kommutativer Ring. Ist R nullteilerfrei, so gilt*

$$(r, a) \sim (s, b) \Longleftrightarrow rb - sa = 0.$$

Satz 4.8.8 *Sei R ein kommutativer Ring und $S \subseteq R$ eine multiplikativ abgeschlossene Menge. Dann ist $(S^{-1}R, +, \cdot)$ ein kommutativer Ring mit $1_{S^{-1}R} = \frac{1}{1}$ und $0_{s^{-1}R} = \frac{0}{1}$, wobei die Addition und die Multiplikation analog zu den entsprechenden Operationen für Brüche definiert sind:*

$$\frac{r}{a} + \frac{s}{b} := \frac{rb + sa}{ab} \text{ und } \frac{r}{a} \cdot \frac{s}{b} := \frac{rs}{ab}.$$

Satz 4.8.9 *Sei R kommutativer Ring und $S \subseteq R$ eine multiplikativ abgeschlossene Teilmenge. Dann ist*

$$\begin{array}{rcl} \iota_S : R & \longrightarrow & S^{-1}R \\ r & \longmapsto & \frac{r}{1} \end{array}$$

ein Ringhomomorphismus mit $\mathrm{Im}(\iota_S \mid S) \subseteq (S^{-1}R)^*$ und $\ker(\iota_S) = \{r \in R \mid \exists s \in S \text{ mit } rs = 0\}$.

Bemerkung 4.8.10 *ι_S ist genau dann injektiv, wenn S weder die Null noch Nullteiler enthält.*
Die Konstruktion des Quotientenkörpers eines Integritätsringes R oben ist gerade die Lokalisierung von R an der multiplikativ abgeschlossenen Menge $S = R \setminus \{0\}$.