Kapitel 4

Äquivalenzrelationen und Faktorstrukturen

Nachdem wir in Kapitel 3 viele Strukturen aus dem ersten Kapitel wieder aufgegriffen und dabei verallgemeinert und formalisiert haben, ist es nun höchste Zeit, eine andere Bringschuld bei Ihnen abzutragen: Auch wenn $\mathbb{Z}_m \cong \mathbb{Z}/m\mathbb{Z}$ bzw. $K[t]_{\leq n} \cong K[t]/\langle h \rangle$ bereits aufgetaucht sind und sie einem Teil von Ihnen auch bereits als Restklassen bekannt sind, werden wir sie hier nochmals von Grund auf einführen. Dabei beginnen wir mit der Frage, was es eigentlich formal bedeuten soll, wenn wir zwei Elemente als äquivalent (bzgl. einer gewissen Eigenschaft) betrachten wollen. Das führt auf den Begriff einer Äquivalenzrelation. Im Kontext von Gruppen und Ringen untersuchen wir dann, darauf basierende Konstruktionen und können dann verschiedene Beispiele, die uns bereits begegnet sind, endlich einordnen.

Die zweite Hälfte des Kapitels ist dann grundlegenden theoretischen Resultaten gewidmet, die sich erst mit Hilfe von Restklassenstrukturen formulieren und beweisen lassen. Insbesondere gewinnen wir eine neue Perspektive auf Bilder von Homomorphismen und auf das Rechnen in $\mathbb{Z}_m$ und lernen darüberhinaus Konstruktionen neuer Körper kennen.

4.1 Äquivalenzrelationen

Vor der Defintion einer Äquivalenzrelation sollten wir uns kurz an die Definition einer Relation erinnern:

Definition 4.1.1 *Sei X eine Menge. Eine* **Relation** *auf X ist eine Teilmenge $\rho \subseteq X \times X$, d.h. ein geordnetes Paar von zwei Elementen aus X. Für ein Paar $(x, y) \in \rho$ sagt man "x steht in Relation zu y", kurz $x \sim_\rho y$ oder $x \sim y$.*

Diese Definition ist sehr abstrakt und insbesondere die Schreibweise als Teilmenge der Menge aller Paare ist nicht ganz intuitiv. Daher auch die alternative Schreibeweise mit $x \sim y$ für "x steht in Relation zu y". Beide Arten der Schreibweise bestehen nebeneinander, ich nutze meist die letztere.

Beispiel 4.1.2 *Betrachten wir die Menge $\mathbb{Z}$, so sind die folgenden Beziehungen Relationen:*

a) x steht in Relation zu y, falls $x > y$.

b) x steht in Relation zu y, falls $x \geq y$.

c) x steht in Relation zu y, falls $x \mid y$.

d) x steht in Relation zu y, falls $x \mid y$ und $y \mid x$, d.h. falls x zu y assoziiert ist.

e) Sei $n \in \mathbb{N}$ fest. x steht in Relation zu y, falls $n \mid x - y$.

Definition 4.1.3 *Sei X eine Menge und ρ eine Relation auf X. ρ heißt*

a) **reflexiv**, *falls $x \sim_\rho x \;\; \forall x \in X$*

b) **symmetrisch**, *falls $(x \sim_\rho y \iff y \sim_\rho x) \;\; \forall x, y, \in X$*

c) **transitiv**, *falls $(x \sim_\rho y$ und $y \sim_\rho z \implies x \sim_\rho z) \;\; \forall x, y, z \in X$*

Eine reflexive, symmetrische und transitive Relation heißt **Äquivalenzrelation**.

Im vorigen Beispiel 4.1.2 erfüllen nicht alle Relationen alle drei Bedingungen. Es hilft sehr beim Verständnis des Begriffs, wenn man die Beispiele und alle drei Eigenschaften einmal in Ruhe durchdenkt oder noch besser mit seinem Abgabepartner durchspricht.

Beispiel 4.1.4 *Bei den Beispielen von oben sehen wir:*

a) $x > y$ *ist transitiv, aber weder reflexiv noch symmetrisch.*

b) $x \geq y$ *ist transitiv und reflexiv, aber nicht symmetrisch.*

c) $x \mid y$ *ist ebenfalls transitiv und reflexiv, aber nicht symmetrisch.*

d) x *assoziiert zu* y *ist transitiv, reflexiv und symmetrisch, also Äquivalenzrelation.*

e) Dies ist ebenfalls eine Äquivalenzrelation, denn $x - x = 0$ *ist durch jede natürliche Zahl teilbar, was die Reflexivität liefert,* $y - x = (-1) \cdot (x - y)$*, woraus die Symmetrie direkt ablesbar ist, und* $x - z = (x - y) + (y - z)$ *ergibt die Transitivität.*

Dazu nun noch zwei weitere Beispiele, bei denen Sie sich die drei Eigenschaften beim Nacharbeiten selbst überlegen sollten, um mit den Begriffen vertrauter zu werden.

f) $x \sim_{2^m} y \quad :\Longleftrightarrow \quad \exists m \in \mathbb{Z} : x = 2^m y.$

g) Seien $A, B \in Mat(n; K)$*.* A *und* B *heißen ähnlich, falls* $\exists P \in GL(n; K) :$ $B = P^{-1}AP$*. Ähnlichkeit von Matrizen ist eine Äquivalenzrelation.*

Sobald man zwei Elemente für äquivalent erklären kann, stellt sich auch die Frage nach allen zu einem Element äquivalenten Elementen und darauf gibt der Begriff der Äquivalenzklasse die Antwort:

Definition 4.1.5 *Sei* X *eine nicht-leere Menge,* $x \in X$ *und* ρ *eine Äquivalenzrelation auf* X*. Dann heißt*

$$[x] := \{y \in X \mid x \sim_\rho y\}$$

die **Äquivalenzklasse** *von* x*.*

Lemma 4.1.6 *Sei* X *eine nicht-leere Menge und* ρ *eine Äquivalenzrelation auf* X*. Dann liegt jedes* $x \in X$ *in genau einer Äquivalenzklasse.*

Beweis: Wir zeigen die Behauptung in zwei Schritten:
Schritt 1: $x \sim_\rho y \implies [x] = [y]$
Sei $z \in [x]$. Dann gilt

$$z \sim_\rho x \overset{x \sim_\rho y, \text{Trans.}}{\Longrightarrow} z \sim_\rho y,$$

weswegen $z \in [y]$ und damit $[x] \subseteq [y]$. Durch Vertauschen der Rollen von x und y folgt dann die andere Inklusion, womit $[x] = [y]$.

Schritt 2: $[x] \cap [y] \neq \emptyset \Longrightarrow [x] = [y]$
Sei $z \in [x] \cap [y]$. Dann gilt $x \sim_\rho z$ und $y \sim_\rho z$, was nach Schritt 1 $[x] = [z] = [y]$ liefert.

□

Bemerkung 4.1.7 *Sei X eine nicht-leere Menge und ρ eine Äquivalenzrelation auf X. Dann kann nach dem vorigen Lemma jede Äquivalenzklasse auf X bzgl. ρ eindeutig durch die Angabe eines Elements der Klasse benannt werden. In diesem Fall sagen wir, dass x ein* **Repräsentant** *der Klasse ist. Die Menge aller Äquivalenzklassen von X bzgl. ρ bezeichnen wir mit $X/\sim_\rho$.*
Die **kanonische** *Projektion von X bzgl. ρ ist die Abbildung*

$$\begin{aligned} \pi : X &\longrightarrow X/\sim_\rho \\ x &\longmapsto [x]. \end{aligned}$$

π ist aufgrund des vorigen Lemmas wohldefiniert und darüberhinaus offensichtlich surjektiv. Eine Teilmenge $\mathcal{O} \subset X$ heißt ein **Repräsentantensystem** *von $X/\sim_\rho$, falls die Einschränkung $\pi|_{\mathcal{O}}: \mathcal{O} \longrightarrow X/\sim_\rho$ bijektiv ist, d.h. falls $\mathcal{O}$ genau einen Repräsentant jeder Klasse bzgl. ρ enthält.*

Notation 4.1.8 *Zwei Menge heißen* **disjunkt**, *wenn ihr Durchschnitt leer ist. Gilt für Mengen X, Y, Z nun $Z = X \cup Y$ und $X \cap Y = \emptyset$, so schreiben wir kurz $Z = X \dot\cup Y$ und nennen Z die disjunkte Vereinigung von X und Y. Eine Zerlegung einer Menge X in eine Vereinigung disjunkter Teilmengen wie im folgenden Korollar nennt man eine* **Partition** *von X.*

Korollar 4.1.9 *Sei X eine nicht-leere Menge, ρ eine Äquivalenzrelation auf X und $\mathcal{O}$ ein Repräsentantensystem bzgl. ρ. Dann gilt*

$$X = \dot{\bigcup_{x \in \mathcal{O}}} [x]$$

Jetzt haben wir formalisiert, was wir unter äquivalent verstehen wollen. Aber noch wissen wir nicht, wozu uns das nützlich sein könnte. Schauen wir uns dazu erst einmal an, was sich an Äquivalenzrelationen direkt anbietet, wenn die zugrundeliegende Menge eine algebraische Struktur trägt.

4.2 Faktorgruppen

Definition 4.2.1 *Sei $(G,+)$ eine abelsche Gruppe und $(U,+) \leq (A,+)$ eine Untergruppe. Die* **Kongruenzrelation** *$T \subset G \times G$ modulo U ist die Relation*

$$(a,b) \in T :\Longleftrightarrow a - b \in U.$$

Für $(a,b) \in T$ schreiben wir $a \equiv b (\mathrm{mod}\, U)$.

Satz 4.2.2 *Sei $(U,+)$ eine Untergruppe einer abelschen Gruppe $(G,+)$. Sei T die Kongruenzrelation modulo U. Dann gilt:*

a) T ist Äquivalenzrelation.

b) Eine Äquivalenzklasse bzgl. T ist von der Form

$$[a] = \{x \in G \mid x \equiv a \,\mathrm{mod}\, U\} = \{x \in G \mid x - a \in U\} =: a + U.$$

c) Bezeichnet G/U die Menge der Äquivalenzklassen modulo U, so ist $(G/U,+)$ eine abelsche Gruppe mit der Gruppenoperation

$$\begin{array}{rcl} + : G/U \times G/U & \longrightarrow & G/U \\ ([a],[b]) & \longmapsto & [a+b] \end{array}$$

Beweis:

a) Für alle $x \in G$ gilt $x - x = 0_G \in U$, weswegen die Kongruzenrelation modulo U reflexiv ist. Ist für $x, y \in G$ bereits $x - y \in U$ erfüllt, so ist auch $y - x = -(x - y) \in U$ da Untergruppen abgeschlossen sind bzgl. der Inversenbildung, womit die Symmetrie der Relation erfüllt ist. Gilt für $x, y, z \in G$ bereits $x - y \in U$ und $y - z \in U$, so ist wegen der Abgeschlossenheit einer Untergruppe bzgl. der Verknüpfung auch $x - z = (x - y) + (y - z) \in U$. Damit ist auch die Transitivität erfüllt und T ist eine Äquivalenzrelation.

b) Die ist lediglich eine explizite Formulierung des Begriffs Äquivalenzklasse in dem konkreten Kontext der Kongruenz modulo U.

c) Seien $[a], [b], [c] \in G/U$ repräsentiert durch $a, b, c \in G$. Aufgrund des Assoziativgesetzes in G muss gelten:

$$([a]+[b])+[c] = [a+b]+[c] = [(a+b)+c] = [a+(b+c)] = [a]+[b+c] = [a]+([b]+[c]),$$

was genau das Assoziativgesetz in U/G liefert. Für alle $[a] \in G/U$, repräsentiert durch $a \in G$, muss gelten:

$$[0_G] + [a] = [0_G + a] = [a],$$

womit $[0_G]$ das neutrale Element in der abelschen Gruppe G/U ist. Für alle $a \in G/U$, repräsentiert durch $a \in G$ gilt weiterhin:

$$[a] + [-a] = [a - a] = [0_G],$$

womit auch die Existenz eines Inversen zu einem gegebenen $[a] \in G/U$ bewiesen ist. Daher ist $(G/U, +)$ eine Gruppe. Diese ist abelsch, da für alle $[a], [b] \in G/U$, reprsentiert durch $a, b \in G$ gilt:

$$[a] + [b] = [a + b] = [b + a] = [b] + [a].$$

□

Beachten Sie, dass wir in diesem Abschnitt nur ablesche Gruppen betrachtet haben. Würden wir auch nicht-abelsche Gruppen G zulassen, so müssten wir deutlich mehr Sorgfalt bei der Wahl von U walten lassen. Dies heben wir uns für die Algebra II auf.

Lemma 4.2.3 *Sei $(U, +)$ eine Untergruppe einer abelschen Gruppe $(G, +)$. Dann ist*

$$\begin{array}{rcl} \varphi : G & \longrightarrow & G/U \\ a & \longmapsto & [a] \end{array}$$

ein Gruppenepimorphismus mit Kern U.

Der Beweis bleibt den Lesern überlassen. Die Wohldefiniertheit von φ folgt bereits aus 4.1.6. Da die Gruppenstruktur auf G/U von der auf G nach Konstruktion induziert ist, folgt auch die Homomorphismuseigenschaft direkt. Die Surjektivität ist ebenfalls direkt nach Konstruktion von G/U gegeben. Bleibt einzig beim Nacharbeiten $ker(\varphi) = U$ nachzurechnen.

4.3 Restklassenringe

Geben wir nun der Menge X aus 4.1 noch etwas mehr Struktur und betrachten Ringe. Dabei helfen uns die bereits für Gruppen gezeigten Eigenschaften, da jeder Ring und jedes Ideal bzgl. der additiven Verknüpfung eine abelsche Gruppe ist. Wir behalten daher auch die dafür eingeführten Schreibweisen bei.

Satz 4.3.1 *Sei R ein Ring und $I \trianglelefteq R$ ein Ideal. Dann ist $(R/I, +, \cdot)$ ein Ring mit Einselement $[1_R]$ bzgl. der Verknüpfungen:*

$$\begin{array}{rcl} + : R/I \times R/I & \longrightarrow & R/I \\ ([a],[b]) & \longmapsto & [a+b] \\ \cdot : R/I \times R/I & \longrightarrow & R/I \\ ([a],[b]) & \longmapsto & [ab] \end{array}$$

Beweis: Aus Satz 4.2.2 wissen wir bereits, dass $(R/I, +)$ eine abelsche Gruppe ist. Der Beweis der Assoziativität bzgl. $\cdot$ erfolgt nach demselben Schema wie bei der Addition: Seien $[a], [b], [c] \in R/I$, repräsentiert durch $a, b, c \in R$:

$$([a] \cdot [b]) \cdot [c] = [a \cdot b] \cdot [c] = [(a \cdot b) \cdot c] = [a \cdot (b \cdot c)] = [a] \cdot [b \cdot c] = [a] \cdot ([b] \cdot [c]).$$

Ebenso sehen wir direkt das Einselement. Sei dazu $[a] \in R/I$ repräsentiert durch $a \in R$:

$$[a] \cdot [1_R] = [a \cdot 1_R] = [a] = [1_R \cdot a] = [1_R] \cdot [a]$$

Für die beiden distributiven Gesetze seien nun $[a], [b], [c] \in R/I$ repräsentiert durch $a, b, c \in R$ und es gilt:

$$([a]+[b])\cdot[c] = [a+b]\cdot[c] = [(a+b)\cdot c] = [a\cdot c+b\cdot c] = [a\cdot c]+[b\cdot c] = ([a]\cdot[c])+([b]\cdot[c])$$

und

$$[a]\cdot([b]+[c]) = [a]\cdot[b+c] = [a\cdot(b+c)] = [a\cdot b+a\cdot c] = [a\cdot b]+[a\cdot c] = ([a]\cdot[b])+([a]\cdot[c]).$$

Im Falle der Kommutativität von R rechnen wir außerdem für $[a], [b] \in R/I$,

repräsentiert durch $a, b, \in R$:

$$[a] \cdot [b] = [a \cdot b] = [b \cdot a] = [b] \cdot [a].$$

□

Definition 4.3.2 *Sei R ein Ring und $I \trianglelefteq R$ ein Ideal. Dann heißt $(R/I, +, \cdot)$ der* **Restklassenring** *(oder* **Faktorring** *von R modulo I.*

Korollar 4.3.3 *Sei R ein Ring und $I \trianglelefteq R$ ein Ideal. Dann ist die kanonische Projektion*

$$\begin{array}{rcl} \pi : R & \longrightarrow & R/I \\ a & \longmapsto & [a] \end{array}$$

ein Ringhomomorphismus mit Kern I.

Jedes Ideal in einem Ring R mit 1 taucht also als Kern eines Ringhomomorphismus auf. Andererseits hatten wir schon in Abschnitt 2.6 gesehen, dass der Kern eines Ringhomomorphismus ein Ideal ist. Einerseits zeigt das, dass Ideale wichtige und interessante Objekte sind. Andererseits sollte hinter diesem Zusammenhang von Idealen und Kernen auch noch mehr stecken. Was genau sehen wir in Abschnitt 4.5. Vorher jedoch werden wir noch ein paar konkrete Restklassenkonstruktionen betrachten.

4.4 Äquivalenzrelationen überall

Die Konstruktion von Äquivalenzrelationen und von Faktorstrukturen kann auf den ersten Blick sehr abstrakt und etwas abgehoben erscheinen, aber wir haben solche Strukturen schon mehrmals gesehen und darin gearbeitet. Andererseits bieten sie uns die Möglichkeit bestimmte Sachverhalte recht kompakt beschreiben zu können.

Der Ring $\mathbb{Z}/m\mathbb{Z}$

In Abschnitt 2.5 waren uns zwei Ringe begegnet:
Einerseits $\mathbb{Z}_m$, dessen Elemente natürliche Zahlen $\{0, 1, \ldots, m-1\}$ sind. Dieser besitzt eine Addition und Multiplikation, die von denen auf $\mathbb{Z}$ dadurch

induziert sind, dass zuerst die Operation in $\mathbb{Z}$ ausgeführt wird und dann der Rest der Division durch m gebildet wird.
Andererseits $\mathbb{Z}/m\mathbb{Z}$, dessen Elemente Restklassen bzgl. des Ideals $\langle m\rangle$ sind. Dieser besitzt eine Addition und Multiplikation die über die Konstruktion eines Restklassenringes induziert sind.
Nachdem wir zu Beginn des Kapitels den Begriff eines Repräsentantensystems kennengelernt habe, stellen wir fest, dass die Menge $\{0, 1, \ldots, m-1\}$ gerade ein Repräsentantensystem von $\mathbb{Z}/m\mathbb{Z}$ ist. Damit haben wir eine $1:1$ Zuordnung zwischen den Elementen der beiden Ringe.
Die Operationen in beiden Ringen werden von denselben Operationen in $\mathbb{Z}$ induziert; der Unterschied besteht lediglich darin, dass wir einmal mit zwei Klassen beginnen und die der Summe oder dem Produkt entsprechende Klasse als Bild erhalten und im anderen Fall mit zwei Repräsentanten starten und als Bild einen Repräsentanten der Klasse des Bildes erhalten. Wir haben uns also gerade in etwas informeller Form überlegt:

$$\begin{array}{rcl} \varphi : (\mathbb{Z}_m, +, \cdot) & \longrightarrow & (\mathbb{Z}/m\mathbb{Z}, +, \cdot) \\ a & \longrightarrow & [a] \end{array}$$

ist ein Isomorphismus von Ringen.

Der Ring $K[t]/\langle h\rangle$

Am Ende von Abschnitt 2.7 begegnete uns eine weiter Konstruktion, die wir in zwei Varianten ausführten:
Einerseits betrachteten wir $K[t]_{\leq n}$, bei dem Addition und Multiplikation von Polynomen vom Grad höchstens n im Polynomring erfolgten und dann durch Division mit Rest bzgl. eines Polynoms h vom Grad $n+1$ wieder auf ein Polynom vom Grad kleiner oder gleich n abgebildet wurden.
Andererseits betrachteten wir $K[t]/\langle h\rangle$ mit den induzierten Operationen als Restklassenring, ohne dies explizit formuliert zu haben.
Wie im vorigen Beispiel existiert eine Isomorphie dieser beiden Ringe (zum selben Polynom h), da die Elemente von $K[t]_{\leq n}$ gerade ein (diesmal in vielen Fällen unendliches) Repräsentantensystem vom $K[t]/\langle h\rangle$ darstellen.

Faktorräume

Nicht nur in Ringen stecken abelsche Gruppen als ein wichtiger Baustein. Schon in der Linearen Algebra haben wir uns mit Vektorräumen befasst,

die bzgl. der inneren Verknüpfung + ebenfalls die Struktur einer abelschen Gruppe tragen und darüberhinaus noch eine Skalarmultiplikation besitzen. Auch auf diese läßt sich die Faktorgruppenkonstruktion anwenden.

Satz 4.4.1 *Sei K ein Körper, V ein K-Vektorraum und U ein Untervektorraum von V. Dann ist V/U ein K-Vektorraum bzgl. der Verknüpfungen*

$$\begin{aligned} + : V/U \times V/U &\longrightarrow V/U \\ ([v],[w]) &\longmapsto [v+w] \\ \cdot : K \times V/U &\longrightarrow V/U \\ (\lambda,[v]) &\longmapsto [\lambda v] \end{aligned}$$

Wie schon zuvor bei Restklassenringen, reicht es zum Beweis der Aussage die Faktorgruppenstruktur bzgl. + zu verwenden und lediglich die Eigenschaften explizit nachzurechnen, die die Skalarmultiplikation betreffen. Dies bietet keinerlei unerwartete Schwierigkeiten oder neue Einsichten und bleibt daher dem interessierten Leser als Teil des Nacharbeitens überlassen.

Korollar 4.4.2 *Sei K ein Körper, V ein K-Vektorraum und U ein Untervektorraum von V. Dann ist die kanonische Projektion*

$$\begin{aligned} \pi : V &\longrightarrow V/U \\ v &\longmapsto [v] \end{aligned}$$

ein K-Vektorraumepimorphismus mit Kern U und es gilt:

$$\dim_K(V/U) = \dim_K(V) - \dim_K(U)$$

Der Beweis der ersten Aussage über den Vektorraumepimorphismus mit Kern U folgt direkt aus der Konstruktion der Abbildung und den bereits gezeigten Eigenschaften des zugrunde liegenden Homomorphismus abelscher Gruppen. Die zweite Aussage ist dann eine direkte Folge aus dem Satz über die Dimension des Kerns und des Bildes einer linearen Abbildung sowie aus dem Wissen um den Kern von π.

Eine kompakte Schreibweise in faktoriellen Ringen

Erinnern wir uns an den Abschnitt über faktorielle Ringe und die dort verwendete Schreibweise für Zerlegung in ein Produkt aus Primelementen:

Erinnerung 4.4.3 *Sei R faktorieller Ring und sei $a \in R \setminus (\{0\} \cup R^*)$. Dann existieren ein $r \in \mathbb{N}$ und Primelemente $c_1, \ldots, c_r \in R$, so dass*

$$a = \prod_{i=1}^{r} c_i.$$

Dabei war explizit nicht ausgeschlossen, dass es Indizes $j_1 \neq j_2$ geben kann mit $cj_1 \sim c_{j_2}$.
Im Fall der Primfaktorzerlegung in den ganzen Zahlen hatten wir daher bereits in der Schule eine etwas andere Formulierung vorgezogen: Sei $a \in \mathbb{Z} \setminus \{0, 1, -1\}$. Dann gibt es ein $s \in \mathbb{N}$, paarweise verschiedene Primzahlen $p_1, \ldots, p_s$ sowie natürliche Zahlen $e_1, \ldots, e_s$, so dass

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

wobei $\varepsilon(a) = \frac{a}{|a|}$ gerade das Vorzeichen von a ist.

Da stellt sich sofort die Frage, ob wir auch in allgemeineren faktoriellen Ringen zueinander assoziierte Faktoren zusammenfassen und die Zerlegung damit eleganter formulieren können.

Erinnerung 4.4.4 *Sei R faktorieller Ring. Dann ist die Assoziiertheit von Elementen nach 4.1.4,d) eine Äquivalenzrelation. Damit können wir für die Äquivalenzklassen ein Repräsentanensystem wählen.*

Nach diesen Überlegungen läßt sich auch die Zerlegung in Primelemente in einem faktoriellen Ring kompakter darstellen:

Bemerkung 4.4.5 *Sei R faktorieller Ring, $a \in R \setminus (\{0\} \cup R^*)$ und $\mathcal{P}$ ein Repräsentantensystem bzgl. Assoziiertheit in R. Dann existieren ein $n \in \mathbb{N}$, Primelemente $p_1, \ldots, p_n \in \mathcal{P}$, $e_1, \ldots, e_n \in \mathbb{N}$ sowie ein $\varepsilon \in R^*$, so dass*

$$a = \varepsilon \prod_{i=1}^{n} p_i^{e_i}.$$

Betrachten wir nun die Exponenten in der obigen Zerlegung noch etwas genauer. Für jedes $a \in R \setminus (\{0\} \cup R^*)$ und jedes Primelement $p \in \mathcal{P}$ läßt sich ein (maximales) $e \in \mathbb{N}_0$ finden, so dass

$$p^e \mid a, \quad \text{aber } p^{e+1} \nmid a.$$

Dieses bezeichnen wir als $v_p(a) := e$. Es beschreibt genau die Vielfachheit des Faktors p in der Zerlegung von a in Primelemente. Damit kann man die Zerlegung von a in Primelemente auch schreiben als:

$$a = \varepsilon \prod_{p \in \mathcal{P} \text{ prim}} p^{v_p(a)}.$$

Direkt fällt in der neuen Schreibweise auf, dass das Produkt möglicherweise unendlich viele Faktoren zu umfassen scheint. Dies täuscht jedoch, da zu einem gegebenen a der Exponent $v_p(a)$ nur für endlich viele Primelemente $p \in \mathcal{P}$ von Null verschieden ist.

Die Wahl der Schreibweise $v_p(a)$ ist kein Zufall. Sie suggeriert bereits, dass es sich hier um Abbildungen handelt.

Definition 4.4.6 *Sei R ein faktorieller Ring und $p \in R$ ein Primelement. Dann definiert*

$$\begin{aligned} v_p : R \setminus \{0\} &\longrightarrow \mathbb{N}_0 \\ a &\longmapsto v_p(a) \end{aligned}$$

mit der oben bereits verwendeten Definition von $v_p(a)$ eine Abbildung.

Die folgenden Eigenschaften sind direkte Konsequenz der Definition der Abbildung v_p:

Lemma 4.4.7 *Sei R faktorieller Ring und $p \in R$ ein Primelement. Dann gilt für alle $a, b \in R \setminus \{0\}$:*

a) $v_p(ab) = v_p(a) + v_p(b)$

b) $v_p(a + b) \geq \min\{v_p(a), v_p(b)\}$

Lemma 4.4.8 *Sei R faktorieller Ring und seien $a, b \in R \setminus \{0\}$. Es gilt:*

a) $b \mid a \iff v_p(b) \leq v_p(a)\ \forall p \in \mathcal{P}$ *prim*

b) $a \in R^* \iff v_p(a) = 0\ \forall p \in \mathcal{P}$ *prim*

Dank der Abbildung v_p läßt sich nun in faktoriellen Ringen auch ein größter gemeinsamer Teiler bzw. ein kleinstes gemeinsames Vielfaches zu zwei von Null verschiedenen Nicht-Einheiten einfach niederschreiben:

Satz 4.4.9 *Sei R faktorieller Ring, $\mathcal{P}$ ein Repräsentantensystem bzgl. der Assoziiertheit in R und seien $a, b \in R \setminus (\{0\} \cup R^*)$. Dann existieren ein größter gemeinsamer Teiler d sowie ein kleinstes gemeinsames Vielfaches k von a und b und es gilt*

$$\begin{aligned} d &= \prod_{p \in \mathcal{P} \text{ prim}} p^{\min(v_p(a), v_p(b))} \\ k &= \prod_{p \in \mathcal{P} \text{ prim}} p^{\max(v_p(a), v_p(b))}. \end{aligned}$$

Ferner gilt: $dk \sim ab$.

Der Beweis beruht auf der Eindeutigkeit der Zerlegung in Primelemente in faktoriellen Ringen (bis auf Reihenfolge und Assoziiertheit). Nach Wahl eines Repräsentantensystems, müssen die primen Faktoren lediglich geeignet eingesammelt werden. Direktes Nachprüfen der Eigenschaften *eines* größten gemeinsamen Teilers bzw. *eines* kleinsten gemeinsamen Vielfachen liefert dann die Behauptung.

4.5 Isomorphiesätze

Wir hatten bereits gesehen, dass jedes Ideal als Kern eines Ringhomomorphismus auftritt und jeder Kern eines Ringhomomorphismus ein Ideal ist. Aber der Zusammenhang zwischen Idealen, Faktorringen und Ringhomomorphismen ist noch deutlich enger, wie wir in diesem Kapitel sehen werden.

Satz 4.5.1 *(Homomorphiesatz) Sei $\varphi : R \longrightarrow S$ ein Ringhomomorphismus. Dann gilt*

$$\begin{aligned} \psi : R/\ker(\varphi) &\longrightarrow \operatorname{Im}(\varphi) \\ [a] &\longmapsto \psi([a]) := \varphi(a) \end{aligned}$$

ist ein Ringisomorphismus.

Beweis:
Schritt 1: Zeige $R/\ker(\varphi)$, $\operatorname{Im}(\varphi)$ Ringe
Aus Satz 2.6.8 wissen wir, dass $\ker(\varphi) \trianglelefteq R$ ein Ideal ist und damit $(R/\ker(\varphi), +, \cdot)$ die von den Verknüpfungen auf R induzierte Ringstruktur trägt. Nach Satz

2.3.7,a) ist $\mathrm{Im}(\varphi)$ ebenfalls ein Ring (natürlich mit $1_{\mathrm{Im}(\varphi)} = 1_S$. Damit ist es überhaupt sinnvoll, über Ringhomomorphismen von $R/\ker$ nach $\mathrm{Im}(\varphi)$ zu sprechen.

Damit wir die Eigenschaften der Zuordnung ψ überhaupt als Abbildung diskutieren können, ist nun der erste Schritt zu zeigen, dass es sich um eine wohldefinierte Abbildung handelt. Erst danach können wir beginnen, zu zeigen, dass ψ ein bijektiver Ringhomomorphismus ist.

Schritt 2: Zeige ψ wohldefiniert
Sei also $[a] \in R/\ker(\varphi)$ eine beliebige Klasse in $R/\ker(\varphi)$ und seien $a_1, a_2 \in R$ zwei Repräsentanten dieser Klasse. Da beide aus der Klasse $[a]$ bzgl. $\ker(\varphi)$ stammen, existiert ein $u \in \ker(\varphi)$, so daß $a_2 = a_1 + u$. Damit rechnen wir:

$$\varphi(a_2) = \varphi(a_1 + u) = \varphi(a_1) + \underbrace{\varphi(u)}_{=0} = \varphi(a_1).$$

Damit ist bewiesen, dass die Wahl des Repräsentanten keinen Einfluß auf $\psi([a]) = \varphi(a_1) = \varphi(a_2)$ hat.

Schritt 3: Zeige ψ Ringhomomorphismus
Seien $a, b \in R$ beliebig. Dann gilt:

$$\begin{aligned} \psi([a] + [b]) = \psi([a + b]) &= \varphi(a + b) = \varphi(a) + \varphi(b) \\ &= \psi[a] + \psi[b] \\ \psi([a] \cdot [b]) = \psi([a \cdot b]) &= \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b) \\ &= \psi[a] \cdot \psi[b]. \end{aligned}$$

Außerdem ist

$$\psi(1_{R/\ker}) = \psi([1_R]) = \varphi(1_R) = 1_S.$$

Damit ist ψ ein Ringhomomorphismus.

Schritt 4: Zeige ψ injektiv
Seien $[a], [b] \in R/\ker(\varphi)$, repräsentiert durch $a, b \in R$ und gelte $\psi[a] = \psi[b]$. Dann gilt:

$$0_{\mathrm{Im}(\varphi)} = \psi([a]) - \psi([b]) = \varphi(a) - \varphi(b) = \varphi(a - b).$$

weswegen $a - b \in \ker(\varphi)$ und damit $[a - b] = [0_R]$, d.h. $[a] = [b]$.

Schritt 5: Zeige ψ surjektiv
Sei $s \in \mathrm{Im}(\varphi)$. Dann exisitiert ein $a \in R$ mit $\varphi(a) = s$. Damit gilt $\psi([a]) = \varphi(a) = s$ und s liegt im Bild von ψ.

Damit haben wir gezeigt, dass es sich bei ψ um einen bijektiven Ringhomomorphismus handelt, also wie behauptet um einen Ringisomorphismus.

□

Satz 4.5.2 *(1. Isomorphiesatz) Sei R ein Ring, $S \leq R$ ein Unterring und $I \trianglelefteq R$ ein Ideal. Dann ist*

$$\begin{array}{rcl} \psi : S/(I \cap S) & \longrightarrow & (I + S)/I \\ [a]_{I\cap S} & \longmapsto & [a]_I \end{array}$$

ein Ringisomorphismus.

Beweis: Auch hier beginnt der Beweis damit, dass zuerst gezeigt werden muss, dass strukturell die Behauptung überhaupt sinnvoll ist. Dazu sollten die beiden Mengen eine Ringstruktur tragen.

Schritt 1: Zeige $I \cap S \trianglelefteq S$ Ideal
Da $S \leq R$ ein Unterring ist und $I \trianglelefteq R$ ein Ideal, enthalten beide 0_R, womit der Schnitt nicht leer ist. Seien nun $a, b \in (I \cap S)$ und $\lambda, \mu \in S$. Dann ist $\lambda a + \mu b \in S$, wegen der Abgeschlossenheit eines Ringes unter Addition und Multiplikation. Andererseits sind λ und $\mu \in S \leq R$ und I ist ein Ideal in R. Daher ist $\lambda a + \mu b \in I$, so dass $\lambda a + \mu b \in I \cap S$. Also ist $I \cap S$ ein Ideal, weswegen dann $S/(I \cap S)$ der Faktorring von S bzgl. $I \cap S$ ist.

Schritt 2: Zeige $I + S \leq R$ Unterring
Da bereits I und S nicht leer sind, ist $I + S$ nicht leer. Seien nun $a + r, b + s \in I + S$. Wir rechnen mittels der Verknüpfungen in R:

$$(a + r) - (b + s) = a + r - b - s = \underbrace{(a - b)}_{\in I} + \underbrace{(r - s)}_{\in S} \subseteq I + S$$

$$(a + r) \cdot (b + s) = \underbrace{ab + as + rb}_{\in I} + \underbrace{rs}_{\in S} \subseteq I + S$$

Damit ist $I+S$ ein Unterring von R, der wegen $0_R \in S$ auch I als $(I+S)$-Ideal enthält. Daher ist $(I+S)/I$ der Faktorring von $I+S$ bzgl. des $(I+S)$-Ideals I.

Schritt 3: Zeige ψ Ringisomorphismus
Betrachte hierzu die beiden Ringhomomorphismen

$$\begin{array}{rcl} \varphi_1: \quad S & \longrightarrow & I+S \\ s & \longmapsto & 0_R + s \text{ und} \\ \varphi_2: I+S & \longrightarrow & (I+S)/I \\ a & \longmapsto & [a]_I. \end{array}$$

Hierbei ist φ_1 ein Ringmonomorphismus und φ_2 ein Ringepimorphismus mit $\ker(\varphi_2) = I \subset I+S$. Die Verkettung

$$\varphi = \varphi_2 \circ \varphi_1 : S \longrightarrow (I+S)/I$$

ist damit ein Ringhomomorphismus. Zum Nachweis der Surjektivität von φ sei $[b] \in (I+S)/I$ beliebig, dann existiert dazu ein Repräsentant $a+s \in I+S$ mit $a \in I$, $s \in S$ und $[a+s]_I = [b]_I$. Damit ist auch $[s]_I = [b]_I$, da $a+s-s = a \in I$. Das bedeutet, dass gilt $[b]_I = \varphi(s)$. Damit ist φ surjektiv. Der Kern von φ besteht genau aus den Elementen $s \in S$, deren Bild $\varphi_1(s)$ unter der ersten Abbildung in I liegt. Dies sind genau die Elemente von $S \cap I$. Damit ist φ ein Ringepimorphismus mit $\ker(\varphi) = I \cap S$ und die Behauptung folgt mit dem Homomorphiesatz.

□

Satz 4.5.3 *(2. Isomorphiesatz) Sei R ein Ring und $I, J \trianglelefteq R$ Ideale mit $J \subseteq I$. Bezeichnet nun I/J das Bild des Ideals I unter der kanonischen Restklassenabbildung bzgl. J, dann ist*

$$\begin{array}{rcl} \psi: (R/J)\,/\,(I/J) & \longrightarrow & R/I \\ [\,[a]_J]_{I/J} & \longmapsto & [a]_I \end{array}$$

ein Ringisomorphismus.

Auch im Beweis des zweiten Isomorphiesatzes geht es um ein sorgfältige Vorbereitung der Anwendung des Homomorphiesatzes auf eine geeignete Abbildung. Der Beweis wird Ihnen als Übungsaufgabe wieder begegnen.