7.1 Ringe und Ideale

Erinnern wir uns zunächst an die Definition von Ringen, es sind Mengen R mit zwei Verknüpfungen $+$ und $\cdot$, so daß $(R,+)$ eine abelsche Gruppe, $(R,\cdot)$ eine Halbgruppe ist, und die beiden Distributivgesetze gelten:

$$r(s+t) = rs + rt,\ (r+s)t = rt + st.$$

Diese Distributivgesetze formuliert man eigentlich besser gleich strukturtheoretisch: Links- und Rechtsmultiplikation mit einem Ringelement ist ein Endomorphismus von $(R,+)$. Das liefert nämlich sofort, daß $0r = r0 = 0$ und $r(-s) = (-r)s = -(rs)$ gelten!

7.1.1 Beispiele

- Ringe, die wir bereits kennengelernt haben sind die Zahlbereiche $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.
- Weitere uns bereits bekannte Beispiele sind die Matrixringe über diesen, also z.B. der Ring $\mathbb{Z}^{n\times n}$, der aus den n-reihigen Matrizen über $\mathbb{Z}$ besteht, mit der Matrixaddition und der Matrizenmultiplikation als Verknüpfungen.
- Allgemeiner gilt: man kann mit einem Ring R und einer nicht leeren Menge M die Menge
$$R^M := \{f \mid f\colon M \to R\}$$
aller Abbildungen von M nach R bilden, die mit punktweiser Addition und Multiplikation,
$$(f+g)(m) := f(m) + g(m),\ (f\cdot g)(m) := f(m)\cdot g(m)$$
offenbar einen Ring bildet.
- Auf solchen Mengen von Abbildungen hat man aber auch Verknüpfungen verwenden, die nicht die punktweisen sind, z.B. ist $R^{\mathbb{N}}$ mit punktweiser Addition und der *Faltung*
$$(f\cdot g)(n) := \sum_{(i,j):i+j=n} f(i)\cdot g(j)$$
identifizierbar mit dem Ring $R[\![x]\!]$ der formalen Potenzreihen über R, in der Unbestimmten x. Der Teilring
$$\left(R^{\mathbb{N}}\right)' := \{f \in R^{\mathbb{N}} \mid \text{ fast alle } f(n) = 0\}$$
ist identifizierbar mit dem Polynomring $R[x]$.
- Daneben bieten die *Endomorphismenringe* abelscher Gruppen eine Fülle an Beispielen: Ist $(A,*)$ abelsche Gruppe, $End(A)$ die Menge ihrer Endomorphismen, dann ist $(End(A),+,\cdot)$ ein Ring mit
$$(f+g)(a) := f(a) * g(a),\ (f\cdot g)(a) := (f\circ g)(a) = f(g(a)).$$

- Wegen der Distributivgesetze ist offensichtlich jeder Ring mit Einselement isomorph zu einem Ring von Endomorphismen von sich selbst, denn man braucht ja nur $r \in R$ auf die Linksmultiplikation mit r abzubilden.

$\diamond$

Ist R ein Ring mit Einselement — und die meisten in der Vorlesung vorkommenden Ringe besitzen ein solches Element —, dann heißt $r \in R$ *Einheit*, wenn es ein $s \in R$ gibt mit $rs = sr = 1$. Die Menge aller Einheiten wird so bezeichnet:

$$E(R) := \{r \in R \mid r \text{ Einheit}\},$$

sie ist eine (multiplikative) Gruppe, die *Einheitengruppe* von R. Einfache Beispiele sind

$$E(\mathbb{Z}) = \{1, -1\},\ E(\mathbb{Z}^{2\times 2}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \pm 1 \right\}.$$

Die tragende Rolle, die in der Gruppentheorie die Normalteiler spielen, übernehmen, wie wir bereits wissen, die Ideale: Eine nicht-leere Teilmenge L von R heißt *Linksideal*, wenn für alle $l, l' \in L$ und alle $r \in R$ gilt:

$$l - l' \in L,\ rl \in L.$$

Analog wurde der Begriff des *Rechtsideals* definiert. Ideale, die sowohl Rechts- als auch Linksideale sind, heißen *(zweiseitige) Ideale,* und wir schreiben hierfür auch

$$I \trianglelefteq R.$$

Ideale sind somit Untermoduln.

Schnitte von Idealen sind ebenfalls Ideale, so daß wir von dem Ideal sprechen können, das von einer Teilmenge $M \subseteq R$ *erzeugt* wird; wir bezeichnen es mit (M). Besteht M aus einem einzigen Element r, dann schreiben wir kurz (r) statt $(\{r\})$. Solche Ideale (r) heißen *Hauptideale*, Ringe, deren Ideale sämtlich Hauptideale sind, dementsprechend *Hauptidealringe*.

7.1.2 Beispiele Ist R ein Ring, dann enthält

- R die *trivialen* Ideale $0 := \{0\}$ und R.
- Für das von $r \in R$ erzeugte Hauptideal gilt:

$$(r) = \left\{ x = \sum_{i=1}^{n} s_i r t_i + rt + ur + zr \;\middle|\; s_i, t_i, u, t \in R, z \in \mathbb{Z}, n \in \mathbb{N} \right\}.$$

  Enthält R ein Einselement, dann reduziert sich dies zu

$$(r) = \left\{ x = \sum_{i=1}^{n} s_i r t_i \;\middle|\; n \in \mathbb{N}, s_i, t_i \in R \right\}.$$

  Ist R zusätzlich kommutativ, dann gilt entsprechend

$$(r) = \{x = sr \mid s \in R\}.$$

- Sind $I, I' \trianglelefteq R$, dann ist deren Summe

$$I + I' = \{x = i + i' \mid i \in I, i' \in I'\}$$

ein Ideal, das *Summenideal*. Analog definieren wir

$$(II') := \left\{ x = \sum_{\nu=1}^{n} i_\nu i'_\nu \;\middle|\; i_\nu \in I, i'_\nu \in I', n \in \mathbb{N} \right\},$$

das *Produktideal*.

- Summen- und Produktideal genügen den folgenden Ungleichungen:

$$(II') \subseteq I \cap I' \subseteq I + I'.$$

◇

Für Ringhomomorphismen, also für Abbildungen $f\colon R \to R'$ zwischen Ringen, mit

$$f(r_0 + r_1) = f(r_0) + f(r_1) \quad \text{und} \quad f(r_0 \cdot r_1) = f(r_0) \cdot f(r_1),$$

sowie $f(1_R) = 1_{R'}$, falls beide Ringe Einselemente besitzen (f nennt man dann manchmal auch genauer einen Ring-mit-Eins-Homomorphismus), gilt, wie wir wissen, der *Homomorphiesatz für Ringe* 2.5.7, welcher insbesondere folgendes impliziert:

- Der Kern ist ein Ideal:

$$\mathrm{Kern}(f) = \{r \in R \mid f(r) = 0_{R'}\} \trianglelefteq R,$$

und zwischen $\mathrm{Bild}(f)$ (einem Ring!) und $\mathrm{Kern}(f)$ besteht die folgende Beziehung:

$$\varphi\colon R/\mathrm{Kern}(f) \simeq \mathrm{Bild}(f)\,,\; r + \mathrm{Kern}(f) \mapsto f(r).$$

- Ist umgekehrt I ein Ideal in R, dann ist dieses der Kern des folgenden Homomorphismus:

$$\nu_I\colon\; R \to R/I, r \mapsto r + I.$$

Ideale sind also genau die Kerne von Ringhomomorphismen!

- Ist I ein Ideal in R, dann erhält man demnach aus der Faktorgruppe $(R/I, +)$ den Faktorring $(R/I, +, \cdot)$ vermöge

$$[r]_I \cdot [s]_I := [rs]_I, \text{ wobei } [r]_I := r + I.$$

Die I entsprechende kanonische Abbildung $\nu_I\colon r \mapsto [r]_I$ auf die Faktorgruppe R/I ist ein Ringepimorphismus mit I als Kern.

7.1.3 Beispiele

- Als *Restklassenring von $\mathbb{Z}$ modulo n* bezeichnen wir den Faktorring
$$(\mathbb{Z}_n, +, \cdot) := (\mathbb{Z}/(n), +, \cdot) = (\mathbb{Z}/n \cdot \mathbb{Z}, +, \cdot).$$
- Ein Ringhomomorphismus zwischen solchen Restklassenringen ist beispielsweise
$$f\colon \mathbb{Z}_{12} \to \mathbb{Z}_3\ ,\ z + (12) \mapsto z + (3).$$
Der Kern ist $(3 + (12))$; da f zusätzlich surjektiv ist, gilt also
$$\mathbb{Z}_{12}/(3 + (12)) \simeq \mathbb{Z}_3.$$
Schreiben wir kurz $n\mathbb{Z}_m$ für das Ideal
$$(n + (m)) = \{0 + (m), n + (m), 2n + (m), \ldots\} \trianglelefteq \mathbb{Z}_m,$$
dann gilt also
$$\mathbb{Z}_{12}/3\mathbb{Z}_{12} \simeq \mathbb{Z}_3.$$

◇

7.1.4 Anwendungen

i) Eine ganz einfache Anwendung der Abbildung von Ringen auf Restklassenringe ermöglicht eine erhebliche Vereinfachung und Parallelisierung beim *Rechnen mit großen ganzen Zahlen:* Der *Chinesische Restesatz* besagt:

- Ist R ein Ring mit Einselement und Idealen $I_0, \ldots, I_{t-1} \trianglelefteq R$. Die Abbildung
$$\varphi\colon R \to \times_{i\in t} R/I_i,\ r \mapsto (r + I_0, \ldots, r + I_{t-1})$$
der Ringelemente auf die Folge ihrer Nebenklassen ist ein Ringhomomorphismus (wenn $\times_{i\in t} R/I_i$ mit punktweiser Addition und Multiplikation versehen ist).
- Sein Kern ist
$$\mathrm{Kern}(\varphi) = \bigcap_{i\in t} I_i,$$
und φ ist genau dann surjektiv, wenn die Ideale paarweise teilerfremd sind:
$$\forall\ i, j \in t, i \neq j\ :\ I_i + I_j = R.$$
- Diese Abbildung φ ist also genau dann ein *Ringisomorphismus,* wenn der Schnitt der Ideale das Nullideal ist und je zwei von ihnen teilerfremd sind.

Nehmen wir beispielsweise $R := \mathbb{Z}$ und $I := (n)$, $I' := (n')$, mit teilerfremden natürlichen Erzeugenden n, n', dann gilt also
$$\mathbb{Z}_{n\cdot n'} \simeq \mathbb{Z}_n \times \mathbb{Z}_{n'}.$$
Das bedeutet: Anstatt in $\mathbb{Z}_{nn'}$ rechnen zu müssen, können wir demnach auch in dem kartesischen Produkt der beiden Restklassenringe rechnen.

ii) Eine Anwendung in der *Analysis* ergibt sich bei der Untersuchung von Nullstellenvarietäten multivariater Polynome:

- Sind $f_0, \ldots, f_{m-1} \in \mathbb{K}[x_0, \ldots, x_{n-1}$ dann bezeichnen wir das von diesen Polynomen erzeugte Ideal mit

$$I(f_0, \ldots, f_{m-1}) := (f_0, \ldots, f_{m-1}).$$

- In der Analysis, genauer: in der algebraichen Geometrie, betrachtet man die zugehörigen polynomialen Funktionen

$$F_i \colon \mathbb{K}^n \to \mathbb{K}\,,\ (x_0, \ldots, x_{n-1}) \mapsto f_i(x_0, \ldots, x_{n-1})$$

  und die zugehörige Varietät

$$V(F_0, \ldots, F_{m-1}) := \{(x_0, \ldots, x_{n-1}) \mid \forall\, i \in m \colon F_i(x_0, \ldots, x_{n-1}) = 0\}.$$

- Man sieht ehr leicht, daß

$$(f_0, \ldots, f_{m-1}) = (g_0, \ldots, g_{l-1}) \Longrightarrow V(F_0, \ldots, F_{m-1}) = V(G_0, \ldots, G_{l-1}).$$

- Zur Varietät $V \subseteq \mathbb{K}^n$ betrachtet man das Ideal (nachprüfen!)

$$I(V) := \{f \in \mathbb{K}[x_0, \ldots, x_{n-1}] \mid \forall\, (x_0, \ldots, x_{n-1}) \in V \colon F(x_0, \ldots, x_{n-1}) = 0\}.$$

- Es gilt ganz offensichtlich

$$(f_0, \ldots, f_{m-1}) \subseteq I(V(f_0, \ldots, f_{m-1})),$$

  aber nicht immer Gleichheit, was allerhand Fragen aufwirft. Beispielsweise gilt

$$(x_0^2, x_1^2) \subset I(V(x_o^2, x_1^2)) = (x, y).$$

Man verwendet dabei insbesondere Gröbnerbasen, das sind Mengen von Polynomen, deren höchste Terme $HT(f_i)$ ein vorgegebenes Ideal erzeugen:

$$(HT(f_0), \ldots, HT(f_{m-1})) = (HT(I)),$$

wobei

$$HT(I) := \{\kappa x^\alpha \mid \exists\, f \in I \colon HT(f) = \kappa x^\alpha\}.$$

Diese Definition hängt allerdings von dem Verständnis ab, was mit *höchster Term* von f gemeint ist, es braucht die Vorgabe einer *Termordnung* (vgl. Übungsblatt). ◇

Besonders interessant sind die beiden folgenden Klassen von Idealen:

- $I \lhd R$ ist *maximales Ideal*, wenn I als Ideal maximal in R ist:

$$\forall\ I' \trianglelefteq R \colon\ [I \subset I' \Rightarrow I' = R]\,.$$

- $I \lhd R$ heißt *Primideal*, wenn $R\backslash I$ multiplikativ abgeschlossen ist, d.h.:

$$(R\backslash I, \cdot) \text{ ist nicht leere Halbgruppe.}$$

Für solche Ideale gilt, wie wir bereits wissen (3.8.10), der wichtige Satz:

- Ist R ein kommutativer Ring mit 1, $I \trianglelefteq R$, dann ist I
  - genau dann Primideal, wenn R/I Integritätsbereich ist,
  - genau dann maximales Ideal, wenn R/I ein Körper ist.

In kommutativen Ringen mit Einselement sind demnach maximale Ideale auch Primideale. In $\mathbb{Z}$ gilt auch die Umkehrung. In vielen Ringen ist das anders, dort klaffen diese Begriffe auseinander, was wiederum heißt, daß die maximalen Ideale und auch die Primideale als *verschiedene* Verallgemeinerungen des Primzahlbegriffs angesehen werden können.

Der gerade wiederholte Satz ist die strukturtheoretische Grundlage für die *Konstruktion von Integritätsbereichen und Zahlkörpern* — auf die wir noch genauer eingehen werden. Maximale Ideale in Polynomringen $\mathbb{K}[x]$ über Körpern $\mathbb{K}$ sind die von irreduziblen Polynomen f erzeugten Hauptideale (f). Alle Restklassenringe $\mathbb{K}[x]/(f)$ sind demnach Erweiterungskörper von $\mathbb{K}$. Wir werden zeigen, daß man auf diese Weise beispielweise alle endlichen Körper aus den sogenannten Primkörpern $\mathbb{Z}_p$, p eine Primzahl, *konstruieren* kann!

Die Existenz maximaler Ideale folgt — ähnlich wie die Existenz von Basen von Vektorräumen — mit dem Lemma von Zorn.