Hauptidealring

Definition Hauptideal

Sei R ein Integritätsring. R heißt *Hauptidealring*, falls jedes Ideal $I \subseteq R$ ein Hauptideal ist, d.h. $I = \langle b \rangle := Rb := \{rb \mid r \in R\}$ für ein $b \in R$.

Satz

Jeder euklidische Ring R ist ein Hauptidealring.

Beweis:

- Falls $I = \{0\}$, gilt $I = \langle 0 \rangle$. Sei also im Folgenden $I \neq \{0\}$.
- Wähle $b \in I$ mit minimaler Bewertungsfunktion $N(b)$.
- Beh.: $I = \langle b \rangle$. Sei $a \in I$ beliebig. Wir müssen $a \in \langle b \rangle$ zeigen.
- Da R euklidisch ist, können wir $a = qb + r$ für $q, r \in R$ schreiben.
- Wegen $r = a - qb$ und $a, b \in I$ folgt $r \in I$.
- Aus $N(r) < N(b)$ und der Minimalität von $N(b)$ folgt $r = 0$.
- Damit gilt $a = qb$ und daher $a \in \langle b \rangle$.

Anmerkung:

Generatoren sind eindeutig bis auf Multiplikation mit Einheiten.

Prim versus irreduzibel

Definition Irreduzibilität

Sei R ein Integritätsbereich und $p \in R \setminus (R^* \cup \{0\})$.

- Wir bezeichnen p als *prim*, falls für alle $r, s \in R$ gilt
$$p|rs \Rightarrow p|r \text{ oder } p|s.$$
- Wir bezeichnen p als *irreduzibel*, falls
$$p = rs \Rightarrow r \in R^* \text{ oder } s \in R^*.$$
- Wir bezeichnen p als *reduzibel*, falls p nicht irreduzibel ist.

Prime Elemente sind irreduzibel.

Satz

Sei R ein Integritätsring und $p \in R$ prim. Dann ist p irreduzibel.

Beweis:

- Sei $p = ab$. Wir müssen zeigen, dass $a \in R^*$ oder $b \in R^*$.
- Da p prim ist, gilt $p|a$ oder $p|b$. OBdA $p|a$.
- Es folgt $pr = a$ für ein $r \in R$. Damit gilt $p = ab = prb$.
- Kürzen von p liefert $rb = 1$ und daher $b \in R^*$.

Irreduzible Elemente müssen nicht prim sein.

Bsp: Wir betrachten $z = 2 + \sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$.

- Wir wollen zunächst zeigen, dass z irreduzibel ist. Wir betrachten
$$N(z) = z\bar{z} = (2 + \sqrt{-5})(2 - \sqrt{-5}) = 2^2 - (-5) = 9.$$
- Sei $r \in \mathbb{Z}[\sqrt{-5}]^*$. Dann gilt $rs = 1$ und
$$N(r)N(s) = N(rs) = N(1) = 1.$$
- Da die Normfunktion nur positive Wert annimmt, folgt $N(r) = 1$.
- D.h. eine nicht-triviale Zerlegung von $z = z_1 z_2$ erfüllt
$$N(z_1) = N(z_2) = 3.$$
- Sei $z_1 = x + y\sqrt{-5}$ mit $N(z_1) = x^2 + 5y^2$.
- Da $x^2 + 5y^2 = 3$ keine Lösung $(x, y) \in \mathbb{Z}^2$ besitzt, existieren in $\mathbb{Z}[\sqrt{-5}]$ keine Elemente mit Norm 3. D.h. z ist irreduzibel.
- Andererseits gilt $z | 3 \cdot 3$ wegen $z \cdot \bar{z} = 9$.
- Gleichzeitig gilt aber $z \nmid 3$. Damit ist z nicht prim in $\mathbb{Z}[\sqrt{-5}]$.

Anmerkung: 9 besitzt in $\mathbb{Z}[\sqrt{-5}]$ zwei verschiedene Faktorisierungen

$$9 = (2 + \sqrt{-5})(2 - \sqrt{-5}) = 3 \cdot 3.$$

Faktorieller Ring

Definition

Sei R ein Integritätsring. R heißt *faktoriell* falls jedes $p \in R \setminus (R^* \cup \{0\})$ in ein Produkt von Primelementen zerlegt werden kann.

Korollar

Sei R faktoriell und $p \in R$ irreduzibel. Dann ist p prim.

Bsp:

- Da p sich nicht weiter zerlegen lässt, aber ein Produkt aus Primelementen ist, muss es selbst prim sein.

Eindeutigkeit der Primelementzerlegung

Satz Eindeutigkeit der Primelementzerlegung

Sei R faktoriell. Dann lässt sich jedes $r \in R$ bis auf Assoziiertheit und Reihenfolge eindeutig in Primelemente zerlegen.

Beweis:

- Seien $r = p_1 p_2 \dots p_n = q_1 q_2 \dots q_m$ zwei Primelementzerlegungen.
- Wegen $p_1 \mid q_1 q_2 \dots q_m$ und p_1 prim, folgt $p_1 \mid q_j$ für ein $j \in [m]$.
- ObdA $p_1 \mid q_1$, d.h. $q_1 = s p_1$. Da q_1 irreduzibel ist, gilt $s \in R^*$.
- Damit sind p_1, q_1 assoziiert. Teilen durch p_1 liefert
$$p_2 p_3 \dots p_n = q_2' q_3 \dots q_m \text{ mit } q_2' = s q_2.$$
- Zeige analog die paarweise Assoziiertheit der restlichen Faktoren.

Anmerkung:
In $\mathbb{Z}[i]$ sind die folgende Zerlegungen äquivalent

$$12 = 3(1+i)^2(1-i)^2 = 3i(1+i)(1-i)^3 \ .$$

Äquivalenzaussagen zu faktoriellen Ringen

Satz Äquivalenzaussagen zu faktoriellen Ringen

Sei R ein Integritätsring und $p \in R \setminus (R^* \cup \{0\})$. Es sind äquivalent:

1. R ist faktoriell.
2. p lässt sich eindeutig in ein Produkt von Primelementen zerlegen. (Eindeutigkeit bis auf Reihenfolge und Assoziiertheit)
3. p lässt sich eindeutig in ein Produkt von irreduziblen Elementen zerlegen. Ferner ist jedes irreduzible Element prim.
4. p lässt sich in ein Produkt von irreduziblen Elementen zerlegen. Ferner ist jedes irreduzible Element prim.

Beweis:

- $1 \Rightarrow 2$: Satz zur Eindeutigkeit der Primelementzerlegung.
- $3 \Rightarrow 4$: trivial.
- $4 \Rightarrow 1$: Definition eines faktoriellen Rings.

Äquivalenzaussagen zu faktoriellen Ringen

Beweis: (Fortsetzung)

- $2 \Rightarrow 3$: Jedes prime Element ist irreduzibel. Damit erhalten wir eine eindeutige Zerlegung jedes Elements in irreduzible Faktoren.
- Bleibt zu zeigen, dass jedes irreduzible Element prim ist.
- Sei r irreduzibel und teile ab, d.h. $rc = ab$. Seien $a = \prod_i a_i$, $b = \prod_j b_j$, $c = \prod_k c_k$ Zerlegungen in irreduzible Faktoren.
- Damit erhalten wir 2 Zerlegungen von ab in irreduzible Faktoren
$$r \prod_k c_k = \prod_i a_i \prod_j b_j.$$
- Aus der Eindeutigkeit der Zerlegung bis auf Reihenfolge und Assoziiertheit ist r zu einem der a_i oder b_j assoziiert.
- D.h. r teilt a oder r teilt b.

Hauptidealringe sind faktoriell.

Satz

Jeder Hauptidealring R ist faktoriell.

Beweis: Wir zeigen Eigenschaft 4 des vorherigen Satzes.

- **Zerlegung in irreduzible Faktoren:** Sei $r \in R \setminus (R^* \cup \{0\})$.
- Solange $r_1 = r$ reduzibel ist, zerlegen wir es weiter.
- Annahme: Zerlegung stoppt nicht, d.h. wir erhalten eine unendliche Kette $r_i = r_{i+1}c$ echter Zerlegungen mit $c \notin R^*$.
- Wegen $r_{i+1} \mid r_i$ und $c \notin R^*$ gilt für die Ideale $\langle r_i \rangle \subset \langle r_{i+1} \rangle$.
- D.h. wir erhalten eine unendlich aufsteigende Kette von Idealen

$$\langle r_1 \rangle \subset \langle r_2 \rangle \subset \langle r_3 \rangle \subset \ldots.$$

- Andererseits ist $I = \bigcup_{i \in \mathbb{N}} r_i$ ein Ideal (Übungsaufgabe).
- Da R ein Hauptidealring ist, gilt $I = \langle r' \rangle$. Wegen $r' \in I$ folgt $r' \in \langle r_i \rangle$ für ein geeignetes i. Damit gilt $\langle r_i \rangle = \langle r_{i+1} \rangle = \ldots$.
- D.h. unsere Kette von Idealen stabilisiert (Widerspruch).

Hauptidealringe sind faktoriell.

Beweis: (Fortsetzung)

- **Jedes irreduzible Element ist prim:** Sei p irreduzibel.
- Sei $p \mid ab$ und $p \nmid a$. Wir müssen zeigen, dass $p \mid b$.
- Betrachte das Ideal $I = \langle p, a \rangle$. Da R ein Hauptideal ist, gilt $I = \langle r \rangle$.
- Wegen $p \in \langle r \rangle$ gilt $p = rc$ und folglich $r \mid p$. Analog gilt $r \mid a$.
- Aus $p = rc$ und der Irreduzibilität von p folgt $r \in R^*$ oder $c \in R^*$.
- Für $c \in R^*$ sind p und r assoziiert, aber $p \nmid a$ und $r \mid a$. (Widerspruch)
- D.h. es muss $r \in R^*$ gelten. Es folgt $I = \langle p, a \rangle = \langle r \rangle = R$.
- Damit können wir jedes Element aus R als Linearkombination von p und a mit Koeffizienten aus R darstellen.
- Insbesondere existieren $x, y \in R$ mit $xp + ya = 1$.
- Multiplikation mit b und Verwendung von $ab = pc'$ liefert

$$xpb + yab = p(xb + yc') = b.$$

- Damit gilt $p \mid b$.