7.3 Euklidische Bereiche, Hauptideal- und Gaußbereiche

Wir wissen bereits, daß in Integritätsbereichen R eine Division mit Rest möglich ist, wenn dort eine *euklidische Norm* existiert, d.h. eine Abbildung $\delta\colon R^* \to \mathbb{N}$ mit

- $\forall\ r, s \in R^* :\ \delta(r) \leq \delta(rs)$,
- $\forall\ x \in R, y \in R^*\ \exists\ q, r \in R :\ [x = qy + r]\ \wedge\ [r = 0 \vee (\delta(r) < \delta(y))]$.

Der Ring R (genauer: das Paar (R, δ)) heißt dann *euklidischer Bereich*.

Eine euklidische Norm auf $\mathbb{Z}$ ist die Betragsfunktion

$$\delta :\ \mathbb{Z}^* \to \mathbb{N},\ z \mapsto |z|,$$

eine Norm auf dem Polynomring $\mathbb{K}[x]$ ist die Gradfunktion

$$\delta :\ \mathbb{K}[x]^* \to \mathbb{N},\ f \mapsto Grad(f).$$

Jeder euklidische Bereich ist ein Hauptidealbereich, denn jedes Element $0 \neq i \in I \trianglelefteq R$ ist durch jedes Element $\neq 0$ und von kleinster Norm teilbar! Demnach ist beispielsweise $\mathbb{Z}$ und jeder Polynomring $\mathbb{K}[x]$ über einem Körper ein Hauptidealring.

Als nächstes wollen wir zeigen, daß in Hauptidealbereichen so etwas wie die im wesentlichen eindeutige Zerlegung ganzer Zahlen in Primfaktoren existiert. Es sei aber gleich betont, daß es zwei wesentlich verschiedene Möglichkeiten gibt, den Begriff Primzahl zu verallgemeinern: Dazu wiederholen wir zunächst die folgenden beiden Bezeichnungen:

- r ist *assoziiert* zu s, wenn es eine Einheit $t \in E(R)$ gibt mit $rt = s$, und das wird wie folgt abgekürzt:

  $$r \sim s.$$

- r ist ein *echter* Teiler von s, wenn folgendes gilt:

  $$r \mid s\ \wedge\ r \notin E(R)\ \wedge\ r \not\sim s.$$

Die beiden Verallgemeinerungen des Begriffs Primzahl sind jetzt:

- r heißt *unzerlegbar*, wenn r weder 0 noch Einheit ist und keine echten Teiler besitzt.
- r heißt *prim*, wenn r weder 0 noch Einheit ist und

  $$r \mid st \Rightarrow [\ r \mid s\ \vee\ r \mid t\ ]$$

  richtig ist, d.h. r teilt mit einem Produkt auch mindestens einen Faktor.

Schließlich sei auch noch betont, daß, für $\emptyset \neq T \subseteq R$, die *Mengen* $\mathrm{ggT}\,(T)$ und $\mathrm{kgV}(T)$ wie folgt definiert wurden: $r \in ggT(T)$, in Worten: r ist *ein größter gemeinsamer Teiler* von T, wenn folgende beiden Bedingungen erfüllt sind:

- $\forall\ t \in T\colon r \mid t$.
- $\forall\ s \in R\colon [\ \forall\ t \in T\colon\ s \mid t\ ] \Rightarrow s \mid r$,

und die Elemente von T heißen genau dann *teilerfremd,* wenn

$$\mathrm{ggT}\,(T) = E(R).$$

$r \in \mathrm{kgV}(T)$, also r ist *ein kleinstes gemeinsames Vielfaches* von T, bedeute, daß

- $\forall\ t \in T\colon\ t \mid r$.
- $\forall\ s \in R\colon\ [\ \forall\ t \in T\colon\ t \mid s\ ] \Rightarrow r \mid s$.

In Integritätsbereichen sind Primelemente stets unzerlegbar. Und wir wissen bereits, daß in Hauptidealbereichen genau die Primelemente unzerlegbar sind. Wir hatten aber auch Beispiele von Integritätsbereichen, wie $\mathbb{K}[x,y] := \mathbb{K}[x][y]$ und $R := \{a + b\sqrt{-5} \mid a,b \in \mathbb{Z}\} \subset \mathbb{C}$, die *keine* Hauptidealbereiche sind.

7.3.1 Definition (Gaußbereich) R sei ein Integritätsbereich mit dem Element r und Nichteinheiten $r_0, \ldots, r_{m-1}$ sowie Nichteinheiten $s_0, \ldots, s_{n-1}$.

- r heißt *streng zerlegbar*, wenn gilt:

$$0 \neq r \notin E(R) \wedge\ r \text{ besitzt echte Teiler.}$$

- $\prod_{i\in m} r_i$ heißt *äquivalent* zu $\prod_{i\in n} s_i$ (kurz: $\prod_i r_i \approx \prod_i s_i$), wenn gilt:

$$m = n\ \wedge\ \exists\ \pi \in S_n\colon\ r_i \sim s_{\pi(i)}.$$

- R heißt *Gaußbereich*, wenn jedes streng zerlegbare Element bis auf Äquivalenz eindeutig als Produkt unzerlegbarer Elemente geschrieben werden kann.

•

Alle Körper sind Gaußbereiche, denn es gibt dort keine streng zerlegbaren Elemente. Unser Ziel ist der Beweis der Tatsache, daß alle Hauptidealbereiche Gaußbereiche sind.

7.3.2 Definition (Kettenbedingungen) Sei $(M, \leq)$ eine angeordnete Menge.

- $(M, \leq)$ genügt der *Maximal-* bzw. der *Minimalbedingung*, wenn jede nichtleere Teilmenge maximale bzw. minimale Elemente enthält.
- $(M, \leq)$ genügt der *Aufsteigende-Ketten-Bedingung* bzw. der *Absteigende-Ketten-Bedingung*, wenn alle aufsteigenden bzw. alle absteigenden Ketten von Elementen stationär werden.

•

7.3.3 Satz *Die Maximalbedingung ist äquivalent zur Aufsteigende-Ketten-Bedingung, die Minimalbedingung ist äquivalent zur Absteigende-Ketten-Bedingung.*

Beweis: Zu einer aufsteigenden Kette

$$m_0 \leq m_1 \leq \dots$$

betrachten wir $\cup_i \{m_i\}$. Gilt die Maximalbedingung, dann gibt es darin maximale Elemente, die Kette muß also stationär werden. Umgekehrt gibt es, wenn keine maximalen Elemente existieren, offensichtlich aufsteigende Ketten, die nicht stationär werden. Entsprechend argumentiert man bei absteigenden Ketten und der Minimalbedingung.

□

7.3.4 Satz *Ist R ein Hauptidealbereich, dann gilt die Aufsteigende-Ketten-Bedingung für die Menge $(\mathcal{I}, \subseteq)$ seiner Ideale.*

Beweis: Ist $I_0 \leq I_1 \leq \dots$ eine aufsteigende Kette von Idealen, dann ist die Vereinigung $I := \cup I_\nu$ ihrer Elemente ein Ideal. R ist Hauptidealbereich, es gibt also $i \in R$ mit $I = (i)$. Dieses i liegt in einem der I_ν, nach diesem Element bleibt die Kette demnach konstant.

□

7.3.5 Satz *Jeder Hauptidealbereich ist Gaußbereich.*

Beweis:

i) Wir beweisen zunächst die *Existenz* der Zerlegung streng zerlegbarer Elemente in unzerlegbare. Sei $r \in R$ streng zerlegbar, R ein Hauptidealbereich. Es gibt also echte Teiler r_0 von r, etwa $r = r_0 r_1$, r_1 ist dann ebenfalls echter Teiler. Wir haben also die beiden Ketten

$$(r) \subset (r_0) \subset R,\ (r) \subset (r_1) \subset R.$$

Der Teiler r_0 von r ist nun entweder unzerlegbar oder streng zerlegbar, in welchem Falle $r_0 = r_{00} r_{01}$ gilt, mit echten Teilern, also insgesamt

$$(r) \subset (r_0) \subset (r_{00}) \subset R,\ (r) \subset (r_0) \subset (r_{01}) \subset R$$

usw., und entsprechend mit r_1. Nun ist aber R ein Hauptidealbereich, so daß (nach 7.3.4) all diese Ketten stationär werden. Die jeweils vorletzten Kettenglieder sind von unzerlegbaren Faktoren von r erzeugt, und das Produkt dieser endlich vielen (!) Faktoren ergibt r.

ii) Um noch die Äquivalenz dieser Faktorisierungen nachzuweisen, betrachten wir zwei Zerlegungen

$$r = p_0 \cdots p_s = q_0 \cdots q_t$$

von r in unzerlegbare Elemente aus R. Da die unzerlegbaren Faktoren auch prim sind, gibt es j mit $p_0 \mid q_j$. Nun ist aber R kommutativ, demnach können wir ohne Einschränkung annehmen, daß $j = 0$ gilt, also, weil auch q_0 unzerlegbar ist,

$$p_0 \sim q_0, \text{ etwa } q_0 = e \cdot p_0, \text{ mit } e \in E(R).$$

Es folgt

$$r' = p_1 \cdots p_s = (e \cdot q_1) \cdots q_t.$$

Ist $s = 1$, dann folgt $t = 1$, und wir sind fertig. Andernfalls argumentieren wir mit p_1 wie oben mit p_0 und erhalten schließlich per Induktion, daß $s = t$ gilt und die beiden Faktorisierungen äquivalent sein müssen.

□

7.3.6 Folgerung *Ist $\mathbb{K}$ ein Körper, dann ist $\mathbb{K}[x]$ ein Gaußbereich.*

Wir haben also insgesamt die folgende Kette von Implikationen (mit den Abkürzungen EB für Euklidischer Bereich, HIB für Hauptidealbereich, GB für Gaußbereich, IB für Integritätsbereich):

7.3.7 Satz *Für Integritätsbereiche R gelten die folgenden Implikationen:*

$$EB(R) \Rightarrow HIB(R) \Rightarrow GB(R) \Rightarrow IB(R).$$

Keine dieser Implikationen ist umkehrbar, das sieht man an:

7.3.8 Beispiele

- Die Menge $\{a + b(\frac{1+\sqrt{-19}}{2}) \mid a, b \in \mathbb{Z}\}$ ist ein Hauptidealbereich, aber kein Euklidischer Bereich. (s. T. Motzkin, *Bull. Amer. Math. Soc.* **55** (1949), 1142-1146)
- Der Polynomring $\mathbb{K}[x, y] := \mathbb{K}[x][y]$ ist ein Gaußbereich (s.u.), aber kein Hauptidealbereich (s. 3.8.11).
- $\{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$ ist ein Integritätsbereich, aber kein Gaußbereich:

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

  die Darstellung als Produkt unzerlegbarer Elemente ist also nicht bis auf Äquivalenz eindeutig (s. 3.8.11).

◇

7.3.9 Satz *In Gaußbereichen sind genau die primen Elemente unzerlegbar.*

Beweis: Primelemente sind unzerlegbar, das haben wir bereits gesehen. Die Umkehrung folgt (indirekter Beweis) so: Sei r unzerlegbar und Teiler von $s \cdot t$, etwa $r \cdot p = s \cdot t$. Nehmen wir an, $r \nmid s$ und $r \nmid t$. Da R Gaußbereich ist, existieren Zerlegungen $s \cdot t = \prod r_i$ und $r \cdot p = r \prod p_i$ in unzerlegbare Elemente, und es gilt: $r \nmid r_i$, also $r \not\sim r_i$, und damit $r \prod p_i \not\approx \prod r_i$, ein Widerspruch.

□

7.3.10 Satz *Sind r, s Elemente eines Gaußbereichs R mit Produktdarstellungen*

$$r \sim \prod_{i=1}^{m} p_i^{m_i},\ s \sim \prod_{i=1}^{m} p_i^{n_i},\ p_i \text{ unzerlegbar},$$

dann besitzen diese Elemente größte gemeinsame Teiler und kleinste gemeinsame Vielfache, es gilt nämlich

$$\prod_{i=1}^{m} p_i^{\min\{m_i,n_i\}} \in ggT(r,s),\ \prod_{i=1}^{m} p_i^{\max\{m_i,n_i\}} \in kgV(r,s).$$

Insgesamt gilt also

$$ggT(r,s) = E(R) \cdot \prod_{i=1}^{m} p_i^{\min\{m_i,n_i\}}$$

und

$$kgV(r,s) = E(R) \cdot \prod_{i=1}^{m} p_i^{\max\{m_i,n_i\}}.$$

Beweis: Übungsaufgabe.

□

7.3.11 Definition (primitive Polynome) Ist R Integritätsbereich, so heißt $f \in R[x]$ genau dann *primitiv*, wenn $Grad(f) > 0$ und die Menge der gemeinsamen Teiler *aller* Koeffizienten von f die Einheiten sind, d.h. wenn

$$E(R) = \text{ggT}\,\{\text{Koeffizienten von } f\}.$$

•

7.3.12 Hilfssatz *Ist R ein Integritätsbereich, $f \in R[x]$ und $r \in R$, dann gilt:*

- $r \mid f \iff r$ *teilt jeden Koeffizienten.*
- $f \in E(R[x]) \iff f \in E(R)$.
- *Ist R Gaußbereich, $Grad(f) > 0$, dann gibt es ein primitives Polynom $g \in R[x]$ und $s \in R$ mit $f = sg$.*
- *Ist $f = r_1 g_1 = r_2 g_2$ mit $r_i \in R$ und primitiven g_i, dann gilt $r_1 \sim r_2$ und $g_1 \sim g_2$.*

Beweis: Übungsaufgabe.

7.3.13 Hilfssatz *Ist R Gaußbereich, dann sind Produkte primitiver Polynome in $R[x]$ primitiv.*

Beweis: Übungsaufgabe.

7.3.14 Satz *Ist R ein Gaußbereich, $\mathbb{K} = B(R, R^*)$ der Quotientenkörper, $f \in R[x]$ primitiv, dann gilt:*

$$f \text{ unzerlegbar in } \mathbb{K}[x] \iff f \text{ unzerlegbar in } R[x].$$

Beweis:

i) Sei $f \in R[x]$ in $\mathbb{K}[x]$ unzerlegbar, es gebe also keinen Teiler $g \in \mathbb{K}[x]$ von f mit $0 < Grad(g) < Grad(f)$. Jeder echte Teiler t von f in $R[x]$ ist also vom Grad 0: $t \in R$. Da f nach Voraussetzung primitiv ist, und t alle Koeffizienten teilt, gilt $t \in E(R)$, d.h. f ist auch in $R[x]$ unzerlegbar.

ii) Sei jetzt f unzerlegbar in $R[x]$ und Produkt $f = gh$ zweier Polynome in $\mathbb{K}[x]$, die echte Teiler seien. Da $\mathbb{K}$ der Quotientenkörper von R ist, gibt es $a, b \in R^*$ mit $ag, bh \in R[x]$. Es gibt demnach primitive $h_1, g_1 \in R[x]$ mit

$$abf = abgh = a_1 b_1 g_1 h_1.$$

Nach 7.3.13 ist deren Produkt $g_1 h_1$ primitiv. Weil f als primitiv vorausgesetzt ist, folgt $f \sim g_1 h_1$, in $R[x]$. Es ergibt sich

$$g_1 \mid f \wedge 0 < Grad(g) = Grad(g_1) < Grad(f).$$

Dies impliziert aber den Widerspruch, g_1 sei ein echter Teiler von f in $R[x]$.

□

7.3.15 Hilfssatz *Ist R Gaußbereich mit Quotientenkörper $\mathbb{K}$ und primitiven Polynomen $f, g \in R[x]$, so gilt*

$$f \sim g \text{ in } R[x] \iff f \sim g \text{ in } \mathbb{K}[x].$$

Beweis:

i) Ist $f \sim g$ in $\mathbb{K}[x]$, etwa $f = eg, e \in E(\mathbb{K}[x]) = \mathbb{K}^*$, dann gibt es $s, t \in R^*$ mit $e = s/t$, also $tf = sg$, was $f \sim g$ impliziert, in $R[x]$.

ii) Die Umkehrung ist trivial.

□

7.3.16 Satz *Polynomringe über Gaußbereichen sind ebenfalls Gaußbereiche.*

Beweis:

i) Ist R Gaußbereich, dann ist R mindestens Integritätsbereich. Bezeichnen wir mit $\mathbb{K}$ den Quotientenkörper, dann ist $\mathbb{K}[x]$ Hauptidealbereich, also Gaußbereich.

ii) Wir beweisen zunächst die *Existenz* von Faktorisierungen streng zerlegbarer Polynome f in unzerlegbare.

1. Sei f ein *primitives* streng zerlegbares Polynom in $R[x]$. Wegen 7.3.14 ist es auch in $\mathbb{K}[x]$ streng zerlegbar, und es gelte dort:

   $$f = \overline{p_1} \cdots \overline{p_s},$$

   mit unzerlegbaren $\overline{p_i}$. Wir wählen $a_i \in R^*$ mit $a_i\overline{p_i} \in R[x]$ und dann $b_i \in R^*$ mit

   $$a_i\overline{p_i} = b_i p_i \in R[x], p_i \text{ primitiv.}$$

   Es gilt dann, für $a := \prod a_i, b := \prod b_i$:

   $$af = bp_1 \cdots p_s.$$

   Nun sind aber auch die p_i unzerlegbar in $\mathbb{K}[x]$. Da sie primitiv sind, sind diese Polynome nach 7.3.14 auch unzerlegbar in $R[x]$. Nach 7.3.13 ist auch deren Produkt primitiv. Da f zu diesem Produkt in $\mathbb{K}[x]$ assoziiert ist, gilt das auch in $R[x]$, nach 7.3.15. Demnach ist f selbst Produkt unzerlegbarer Polynome aus $R[x]$.

2. Sei $f \in R[x]$ jetzt *irgendein* streng zerlegbares Polynom in $R[x]$. Wir unterscheiden zwei Fälle:

   a) Ist $f \in R$, dann gibt es, da R Gaußbereich ist, unzerlegbare a_i mit $f = a_1 \cdots a_h$. Eine solche Zerlegung ist in R bis auf Äquivalenz eindeutig, also auch in $R[x]$. Bei $f \in R$ gilt also die Behauptung.

   b) Ist $f \notin R$, dann gibt es $d \in R^*$ mit $f = dg$ und einem primitiven $g \in R[x]$. Wie unter 1. ergeben sich Zerlegungen $g = p_1 \cdots p_s,\ d = d_1 \cdots d_h$, also auch Faktorisierungen von f:

   $$f = d_1 \cdots d_h p_1 \cdots p_s.$$

iii) Zum Beweis der *Äquivalenz* zweier solcher Zerlegungen betrachten wir

$$f = d_1 \cdots d_h p_1 \cdots p_s = e_1 \cdots e_k q_1 \cdots q_t,$$

mit unzerlegbaren $d_i, e_i \in R$, und unzerlegbaren $p_i, q_i \in R[x]\backslash R$, von denen wir ohne Einschränkung annehmen können, sie seien zusätzlich auch primitive Polynome. Es gilt dann

$$d_1 \cdots d_h \sim e_1 \cdots e_k, \text{ in } R.$$

Da R Gaußbereich ist, impliziert dies die Äquivalenz dieser beiden Produkte. Die Produkte $d_1 \cdots d_h$ und $e_1 \cdots e_k$ sind dann auch in $R[x]$ äquivalent, insbesondere gilt $h = k$.
Auch die polynomialen Faktoren $p_1 \cdots p_s$ und $q_1 \cdots q_t$ sind assoziiert in $R[x]$, also auch in $\mathbb{K}[x]$, dies ist aber ein Gaußbereich, also sind sie dort sogar äquivalent, und insbesondere gilt $s = t$. Geeignete Paare sind also assoziiert in $\mathbb{K}[x]$, nach 7.3.15 auch assoziiert in $R[x]$, so daß diese beiden Produkte sogar in $R[x]$ äquivalent sind. Insgesamt ergibt sich daraus die Äquivalenz der beiden Faktorisierungen von f.

□

Wiederholte Anwendung dieses Satzes ergibt

7.3.17 Folgerung *Ist R ein Gaußbereich, $n \in \mathbb{N}$, dann ist der Polynomring*

$$R[x_1, \ldots, x_n] := R[x_1, \ldots, x_{n-1}][x_n]$$

ein Gaußbereich.

7.3.18 Unzerlegbarkeitskriterien *Sei R ein Integritätsbereich, dann gilt im Polynomring $R[x]$:*

- *Die linearen Polynome $f = r + sx, s \in E(R)$, sind sämtlich unzerlegbar.*
- *Für alle $r \in R$ ist $f(x) \in R[x]$ genau dann unzerlegbar, wenn $f(x + r)$ unzerlegbar ist.*
- *Ist R sogar Gaußbereich, $f \in R[x]$ primitiv, dann ist f, als Polynom über $\mathbb{K} = B(R, R^*)$, genau dann unzerlegbar, wenn f auch über R unzerlegbar ist.*
- *Ist $R = \mathbb{Z}$, $f \in \mathbb{Z}[x]$ primitiv und unzerlegbar über $\mathbb{Z}_p$ (genauer: $\overline{f}$, das aus f durch Reduktion der Koeffizienten modulo p hervorgeht) und teilt p den Leitkoeffizienten nicht, dann ist f auch in $\mathbb{Z}[x]$ unzerlegbar.*
- Kriterium von Eisenstein: *Ist R Gaußbereich, $f = \sum_{i=0}^{n} a_i x^i \in R[x]$ primitives Polynom, $p \in R$ ein Primelement, für das in R gilt:*

  $$p \nmid a_n, p \mid a_{n-1}, p \mid a_{n-2}, \ldots, p \mid a_0, p^2 \nmid a_0,$$

  dann ist f über R unzerlegbar.

Beweis: Das Eisensteinkriterium zeigen wir indirekt: Ist $f = \sum a_i x^i = gh$, mit $g = \sum b_i x^i, h = \sum c_i x^i$, dann teilt p entweder b_0 nicht oder c_0 nicht, o.E. $p \nmid c_0$. Da p kein Teiler von a_n ist, gibt es einen kleinsten Index i mit $p \nmid b_i$. Nun ist aber

$$a_i = b_i c_0 + (b_{i-1} c_1 + \ldots + b_0 c_i),$$

wobei p den eingeklammerten Summanden auf der rechten Seite teilt, aber nicht $b_i c_0$, also auch nicht a_i. Damit ist $i = n$, und der Grad von h ist Null. Da f als primitiv vorausgesetzt war, ist $h \in E(R)$.

□

Das Eisensteinkriterium veranlaßt uns zu folgender

7.3.19 Definition (irreduzible Polynome) Ein Polynom $f \in R[x]^*$, R Gaußbereich, heißt *irreduzibel*, wenn für $g, h \in R[x]$ gilt:

$$[f = gh \;\Rightarrow\; Grad(g) = 0 \;\vee\; Grad(h) = 0]$$

•

Im Falle, daß f primitiv oder R ein Körper ist, sind Unzerlegbarkeit und Irreduzibilität gleichwertig.

7.3.20 Beispiele

- $f(x) := 2+4x+6x^2+4x^3+x^4 = (x+1)^4+1$ ist über $\mathbb{Z}$ unzerlegbar nach dem Eisensteinkriterium, damit ist y^4+1 unzerlegbar über $\mathbb{Q}$.
- $f := -135+17x-8x^2+x^3$ ergibt, modulo $p=2$, das Polynom $\overline{f} = 1+x+x^3 \in \mathbb{Z}_2[x]$, das dort unzerlegbar ist, denn eine Zerlegung müßte einen Linearfaktor enthalten, $1+x+x^3$ also eine Nullstelle besitzen, was offensichtlich nicht der Fall ist. Also ist $f \in \mathbb{Z}[x]$ irreduzibel.
- Mit Hilfe einer Kombination des Eisensteinkriteriums mit dem Transformationskriterium ergibt sich auch die Unzerlegbarkeit der wichtigen *Kreisteilungspolynome*

  $$\Phi_p(x) := \frac{x^p-1}{x-1} = x^{p-1}+x^{p-2}+\ldots+1 \in \mathbb{Z}[x],$$

  für Primzahlen p. Denn

  $$\Phi_p(x+1) = x^{p-1}+\binom{p}{1}x^{p-2}+\binom{p}{2}x^{p-3}+\ldots+\binom{p}{p-1}$$

  ist unzerlegbar nach dem Eisensteinkriterium.

$\diamond$