UNTERLAGEN ZUR TEILBARKEIT IN KOMMUTATIVEN RINGEN

VORLESUNG "KOMMUTATIVE ALGEBRA", SOMMERSEMESTER 2007

1. Definitionen

Ein kommutativer Ring mit Eins R ist ein *Integritätsbereich*, wenn er zumindest zwei Elemente hat und für alle a, b mit $a \neq 0$ und $b \neq 0$ auch $ab \neq 0$ gilt.

Definition 1.1. Sei R ein kommutativer Ring mit Eins, und seien $a, b \in R$. Dann gilt $a|b$, wenn es ein $r \in R$ gibt, sodass $b = ra$.

Definition 1.2. Sei R ein kommutativer Ring mit Eins.

- Ein Element $u \in R$ ist *invertierbar*, wenn es ein $v \in R$ mit $uv = 1$ gibt.
- Ein Element $p \in R$ ist *prim*, wenn es nicht invertierbar ist, und für alle $a, b \in R$ mit $p|ab$ gilt: $p|a$ oder $p|b$.
- Ein Element $r \in R$ ist *irreduzibel*, wenn es nicht invertierbar ist, und für alle $s, t \in R$ mit $r = st$ gilt: s ist invertierbar oder t ist invertierbar.
- Zwei Elemente $a, b \in R$ sind *assoziiert*, wenn es ein invertierbares Element $u \in R$ gibt, sodass $au = b$. Wir schreiben dann $a \sim b$ oder $a \sim_R b$.

Lemma 1.3. *Sei R ein Integritätsbereich, und sei p ein primes Element von R mit $p \neq 0$. Dann ist p irreduzibel.*

Beweis: Sei p prim, $p \neq 0$, und seien $s, t \in R$ so, dass $p = st$. Dann gilt $p|st$. Da p prim ist, gilt $p|s$ oder $p|t$. Im Fall $p|s$ gibt es ein $s_1 \in R$, sodass $ps_1 = s$. Durch Multiplikation dieser Gleichung mit t erhalten wir $ps_1t = st = p$. Also gilt $p(s_1t - 1) = 0$. Wegen $p \neq 0$ ist also t invertierbar. Im Fall $p|t$ erhalten wir analog, dass s invertierbar ist. □

2. Faktorielle Integritätsbereiche

Definition 2.1. Sei R ein Integritätsbereich. R ist *faktoriell*, wenn folgendes gilt:

Date: March 26, 2007.

Erhard Aichinger, Institut für Algebra, Johannes Kepler Universität Linz, Austria, erhard@algebra.uni-linz.ac.at.

(1) Für alle $r \in R \setminus \{0\}$, die nicht invertierbar sind, gibt es ein $s \in \mathbb{N}$ und irreduzible $f_1, \ldots, f_s \in R$, sodass
$$r = f_1 \cdots f_s.$$
(2) Für alle $m, n \in \mathbb{N}$ und für alle irreduziblen $f_1, \ldots, f_m, g_1, \ldots, g_n \in R$ mit
$$f_1 \cdots f_m = g_1 \cdots g_n$$
gilt $m = n$, und es gibt eine bijektive Abbildung $\pi : \{1, \ldots, m\} \to \{1, \ldots, n\}$, sodass für alle $i \in \{1, \ldots, m\}$ gilt: $f_i \sim_R g_{\pi(i)}$.

Lemma 2.2. *Sei R ein faktorieller Integritätsbereich. Dann ist jedes irreduzible Element prim.*

Beweis: Sei f irreduzibel, und seien $a, b \in R$ so, dass $f|ab$. Zu zeigen ist, dass f mindestens eines der Elemente a oder b teilt. Wegen $f|ab$ gibt es $r \in R$, sodass
$$fr = ab.$$
Wenn $a = 0$, so gilt $f|a$; wenn $b = 0$, so gilt $f|b$. Wir nehmen nun an, dass $a \neq 0$ und $b \neq 0$. Wenn a invertierbar ist, dann gilt $fra^{-1} = b$, und somit $f|b$; wenn b invertierbar ist, gilt $f|a$. Es bleibt der Fall, dass a, b beide $\neq 0$ und beide nicht invertierbar sind. Dann gibt es $m, n \in \mathbb{N}$ und irreduzible Elemente $a_1, \ldots, a_m, b_1, \ldots, b_n \in R$, sodass
$$a = a_1 \cdots a_m \text{ und } b = b_1 \cdots b_n.$$
Falls r invertierbar ist, dann ist fr irreduzibel, und wegen der Eindeutigkeit der Zerlegung zu einem a_i oder b_j assoziiert. Wenn fr zu einem a_i assoziiert ist, dann gilt $fr|a$, und somit $f|a$; wenn fr zu einem b_j assoziiert ist, dann gilt $f|b$.

Wenn r nicht invertierbar ist, dann gibt es $l \in \mathbb{N}$ und irreduzible Elemente $r_1, \ldots, r_l \in R$, sodass
$$fr_1 \cdots r_l = a_1 \cdots a_m \cdot b_1 \cdots b_n.$$
Wegen der Eindeutigkeit der Zerlegung ist f zu einem a_i oder b_j assoziiert. Es gilt also wieder $f|a$ oder $f|b$. □

3. Zerlegung in irreduzible Elemente

Definition 3.1. Sei R ein Integritätsbereich, und sei $I \subseteq R$. I ist eine *vollständige Auswahl irreduzibler Elemente*, wenn alle $i \in I$ irreduzibel sind, und es für jedes irreduzible $f \in R$ genau ein $i \in I$ mit $f \sim_R i$ gibt.

Definition 3.2 (Zerlegung)**.** Sei R ein Integritätsbereich, und sei $I \subseteq R$ eine vollständige Auswahl irreduzibler Elemente von R. Sei $a \in \mathbb{R}\setminus\{0\}$. Eine Funktion $\alpha : I \to \mathbb{N}_0$ ist eine *Zerlegung* von a, wenn

(1) $\{i \in I \,|\, \alpha(i) \neq 0\}$ ist endlich.

(2) $a \sim_R \prod_{i\in I} i^{\alpha(i)}$.

Dabei definieren wir für alle $i \in I$, dass $i^0 := 1$ ist. Ebenso ist ein Produkt $\prod_{i\in\emptyset}$ immer gleich 1.

Lemma 3.3. *Sei R ein faktorieller Integritätsbereich und sei I eine vollständige Auswahl irreduzibler Elemente von R. Seien $a, b \in R \setminus \{0\}$, sei α eine Zerlegung von a bezüglich I und β eine Zerlegung von b bezüglich I. Dann sind äquivalent:*

(1) *$a|b$.*
(2) *Für alle $i \in I$ gilt $\alpha(i) \leq \beta(i)$.*

Beweis: Wir beweisen nur (1)⇒(2). Sei $r \in R$ so, dass $ar = b$. Wir nehmen an, dass es ein $i_0 \in I$ gibt, sodass $\alpha(i_0) > \beta(i_0)$. Dann gilt

$$r \cdot i_0^{\alpha(i_0)} \cdot \prod_{\substack{i\in I\\ i\neq i_0}} i^{\alpha(i)} \sim_R i_0^{\beta(i_0)} \cdot \prod_{\substack{i\in I\\ i\neq i_0}} i^{\beta(i)}.$$

Es gibt also ein invertierbares $u_1 \in R$, sodass

$$u_1 \cdot r \cdot i_0^{\alpha(i_0)} \cdot \prod_{\substack{i\in I\\ i\neq i_0}} i^{\alpha(i)} = i_0^{\beta(i_0)} \cdot \prod_{\substack{i\in I\\ i\neq i_0}} i^{\beta(i)}.$$

Da R ein Integritätsbereich ist und $i_0^{\beta(i_0)} \neq 0$, gilt

$$u_1 \cdot r \cdot i_0^{\alpha(i_0)-\beta(i_0)} \prod_{\substack{i\in I\\ i\neq i_0}} i^{\alpha(i)} = \prod_{\substack{i\in I\\ i\neq i_0}} i^{\beta(i)}.$$

Der Ring R ist faktoriell. Also gibt es ein invertierbares Element $u_2 \in R$ und ein $s \in \mathbb{N}_0$ und irreduzible Elemente $r_1, \ldots, r_s \in R$ sodass $r = u_2 r_1 \cdots r_s$. Es gilt dann

$$u_1 u_2 r_1 \cdots r_s \cdot i_0^{\alpha(i_0)-\beta(i_0)} \prod_{\substack{i\in I\\ i\neq i_0}} i^{\alpha(i)} = \prod_{\substack{i\in I\\ i\neq i_0}} i^{\beta(i)}. \tag{3.1}$$

Falls $\{i \in I \,|\, \beta(i) > 0 \text{ und } i \neq i_0\} = \emptyset$, so ist i_0 invertierbar, im Widerspruch dazu, dass i_0 irreduzibel ist. Wenn die rechte Seite von (3.1) aus einer positiven Anzahl von Faktoren besteht, können wir verwenden, dass R faktoriell ist. Wir erhalten dann ein $i_1 \in I$ mit $i_1 \neq i_0$ und $i_1 \sim_R i_0$. Das ist unmöglich, da I keine verschiedenen assoziierten Elemente enthält. □

Lemma 3.4 (Eindeutigkeit der Zerlegung)**.** *Sei R ein faktorieller Integritätsbereich und sei I eine vollständige Auswahl irreduzibler Elemente von R. Sei $f \in R\setminus\{0\}$. Dann gibt es genau eine Zerlegung $\alpha : I \to \mathbb{N}_0$ von f.*

Beweis: Wir zeigen zunächst, dass es ein α mit den geforderten Eigenschaften gibt. Wenn f invertierbar ist, so definieren wir α durch $\alpha(i) = 0$ für alle $i \in I$. Es gilt $f \sim_R 1$, also ist (2) aus Definition 3.2 erfüllt. Wenn f nicht invertierbar ist, so gibt es $s \in \mathbb{N}$ und irreduzible Elemente $g_1, \ldots, g_s \in R$, sodass

$$f = g_1 \cdots g_s.$$

Seien nun $i_1, \ldots, i_s \in I$ und $u_1, \ldots, u_s$ invertierbare Elemente von R, sodass für alle $j \in \{1, \ldots, s\}$ gilt: $g_j = u_j i_j$. Es gilt dann $f = (u_1 \cdots u_s) \cdot (i_1 \cdots i_s)$. Für $i \in I$ definieren wir $\alpha(i)$ als die Anzahl der Elemente von $\{j \in \{1, \ldots, s\} \mid i_j = i\}$. Um die Eindeutigkeit zu zeigen, fixieren wir $\alpha, \beta : I \to \mathbb{N}_0$, sodass beide Funktionen nur an endlich vielen Stellen nicht 0 sind, und

$$\prod_{i \in I} i^{\alpha(i)} \sim_R \prod_{i \in I} i^{\beta(i)}.$$

Wegen Lemma 3.3 gilt dann $\alpha = \beta$. □

Satz 3.5. *Sei R ein Integritätsbereich. Dann sind äquivalent:*

(1) *R erfüllt die ACC für Hauptideale, und jedes irreduzible Element von R ist prim.*
(2) *R ist faktoriell.*

Beweis: (1)⇒(2). Wir zeigen zunächst, dass sich jedes nicht invertierbare Element $r \neq 0$ in ein Produkt von irreduziblen Elementen zerlegen lässt. Dazu nehmen wir an, dass es ein nicht invertierbares Element $r \neq 0$ gibt, das sich nicht zerlegen lässt. Wir wählen $r \in R \setminus \{0\}$ so, dass (r) maximal in der Menge

$$\{(r') \mid r' \text{ ist nicht invertierbar und nicht Produkt von irreduziblen Elementen}\}$$

ist. Da r nicht invertierbar ist, gilt $(r) \neq R$. Nun wählen wir $s \in R$ so, dass (s) maximal in der Menge

$$\{(s') \mid (r) \subseteq (s') \neq R\}$$

ist. Wir zeigen als erstes, dass s irreduzibel ist. Wenn $s = s_1 s_2$, so gilt $(s) \subseteq (s_1)$ und $(s) \subseteq (s_2)$. Wenn s_1 nicht invertierbar ist, so gilt wegen der Maximalität von (s) die Gleichheit $(s) = (s_1)$. Folglich gibt es $t \in R$, sodass $s_1 = ts$, also $s_1 = ts_1 s_2$. Da $s_1 \neq 0$, ist s_2 invertierbar. Somit ist s irreduzibel. Da $r \in (s)$, gibt es $t_1 \in R$, sodass $r = t_1 s$. Wenn t_1 invertierbar ist, so ist r irreduzibel, im Widerspruch zur Wahl von r. Wenn t_1 nicht invertierbar ist, so gilt $(r) \subseteq (t_1) \neq R$. Wenn nun $(r) = (t_1)$, so gibt es ein $s_1 \in R$ mit $t_1 = s_1 r = s_1 t_1 s$. Da $t_1 \neq 0$, ist dann $s_1 s = 1$ und s somit invertierbar. Also gilt $(r) \neq (t_1)$. Wegen der Maximalität von (r) lässt sich t_1 als Produkt von irreduziblen Elemente schreiben. Fügen wir zu diesem Produkt noch s dazu, haben wir auch r als Produkt irreduzibler Elemente geschrieben, im Widerspruch zur Wahl von r. Somit lässt sich jedes nicht invertierbare Element $\neq 0$ in irreduzible Elemente zerlegen.

Nun zeigen wir die Eindeutigkeit. Seien $m, n \in \mathbb{N}$, und $f_1, \ldots, f_m, g_1, \ldots, g_n$ irreduzible Elemente, sodass $f_1 \cdots f_m = g_1 \cdots g_n$. Wir zeigen durch Induktion nach $\min(m, n)$, dass sich die f_i und g_j zueinander assoziieren lassen. Wenn $m = 1$, so gilt, da f_1 irreduzibel ist, auch $n = 1$, und somit $f_1 = g_1$. Wenn $n = 1$, so gilt analog $m = 1$ und $f_1 = g_1$. Wenn $m \geq 2$ und $n \geq 2$, dann gilt $f_1 | g_1 \cdots g_n$. Da f_1 nach Voraussetzung prim ist, teilt es eines der g_i. Da g_i irreduzibel ist, gilt $f_1 \sim_R g_i$. Wir wenden nun die Induktionsvoraussetzung auf $f_2 \cdots f_m = g_1 \cdots g_{i-1} g_{i+1} \cdots g_n$ an.

(2)⇒(1): Sei R ein faktorieller Ring, und sei $(a_1) \subseteq (a_2) \subseteq (a_3) \subseteq \ldots$ eine Kette von Hauptidealen. Wir nehmen an $(a_1) \neq (0)$. Dann gilt $a_n | a_{n-1} | \cdots | a_3 | a_2 | a_1$. Sei I eine vollständige Auswahl von irreduziblen Elementen, und sei α_k eine Zerlegung von a_k bezüglich I. Es gilt dann nach Lemma 3.3 für alle $i \in I$: $\alpha_k(i) \leq \alpha_1(i)$. Da es nur endlich viele β mit der Eigenschaft $\beta(i) \leq \alpha_1(i)$ für alle $i \in I$ gibt, gibt es ein $N \in \mathbb{N}$, sodass für $k \geq N$ gilt: $\alpha_k = \alpha_N$. Dann gilt aber auch $(a_k) = (a_N)$. Dass jedes irreduzible Element prim ist, folgt aus Lemma 2.2. □

Definition 3.6. Ein Integritätsbereich R ist ein *Hauptidealbereich*, wenn es für jedes Ideal I von R ein $a \in R$ gibt, sodass $I = (a)$.

Satz 3.7. *Jeder Hauptidealbereich ist faktoriell.*

Beweis: Sei R ein Hauptidealbereich. Da jedes Ideal von R endlich erzeugt ist, erfüllt R die ACC für Ideale, also insbesondere für Hauptideale. Zu zeigen bleibt, dass jedes irreduzible Element von R prim ist. Sei r ein irreduzibles Element von R, und sei P ein maximales Ideal von R mit $(r) \subseteq P \neq R$. Da R ein Hauptidealbereich ist, gibt es $p \in R$, sodass $P = (p)$. Da $r \in (p)$, gibt es ein $s \in R$, sodass $r = s \cdot p$. Da r irreduzibel ist und $(p) \neq R$, kann von s und p nur s invertierbar sein. Da s invertierbar ist, gilt $(p) = (r)$. Das Ideal (r) ist also ein maximales Ideal von R. Somit ist $R/(r)$ ein Körper, also auch ein Integritätsbereich, und (r) ist damit prim. □

4. Eine Anwendung auf die Zahlentheorie

Wir beweisen in dieser Sektion den folgenden Satz:

Satz 4.1. *Sei p eine Primzahl mit $p \equiv 1 \pmod 4$. Dann gibt es $a, b \in \mathbb{N}$, sodass $a^2 + b^2 = p$.*

Wir werden im Beweis den Ring der Gaußschen ganzen Zahlen, einen Unterring des Körpers der komplexen Zahlen, der durch

$$\mathbb{Z}[i] := \{a + b\,i \mid a, b \in \mathbb{Z}\},$$

definiert ist, verwenden.

Lemma 4.2. *Der Ring $\mathbb{Z}[i]$ ist ein Hauptidealring.*

Beweis: Für jedes Element $a+b\,i \in \mathbb{Z}[i]$ definieren wir seine Norm durch $N(a+b\,i) := a^2+b^2$. Aus $N(z) = z\overline{z}$ sieht man leicht, dass $N(z_1z_2) = N(z_1)N(z_2)$ für alle $z_1, z_2 \in \mathbb{Z}[i]$ gilt. Sei nun I ein Ideal von $\mathbb{Z}[i]$ mit $I \neq \{0\}$. Wir wählen ein Element $c+d\,i$ aus $I \setminus \{0\}$, für das $N(c+d\,i)$ minimal ist. Nun zeigen wir

$$I = \{\lambda_1(c+d\,i) + \lambda_2(-d+c\,i) \mid \lambda_1, \lambda_2 \in \mathbb{Z}\}. \tag{4.1}$$

Die Inklusion $\supseteq$ folgt daraus, dass $(\lambda_1+\lambda_2\,i)(c+d\,i)$ in I liegt. Um $\subseteq$ zu beweisen, wählen wir einen Punkt $a+b\,i \in I$. Es gibt einen Vektor in $\{\lambda_1 \begin{pmatrix} c \\ d \end{pmatrix} + \lambda_2 \begin{pmatrix} -d \\ c \end{pmatrix} \mid \lambda_1, \lambda_2 \in \mathbb{Z}\}$, dessen Abstand von $\begin{pmatrix} a \\ b \end{pmatrix}$ höchstens $\frac{1}{\sqrt{2}}\sqrt{c^2+d^2}$ ist. Sei $\begin{pmatrix} c' \\ d' \end{pmatrix}$ ein solcher Vektor. Da $c'+d'\,i \in I$ liegt, liegt auch $(a-c')+(b-d')\,i$ in I. Es gilt $N((a-c')+(b-d')\,i) \leq \frac{1}{2}(c^2+d^2)$. Da $c+d\,i$ minimale Norm in I hat, gilt $(a-c')+(b-d')\,i = 0$. Somit liegt $a+b\,i$ in der rechten Seite von (4.1). □

Wir beweisen nun Satz 4.1:

Beweis von Satz 4.1: Wir zeigen als erstes, dass es ein $x \in \mathbb{Z}$ gibt, sodass

$$x^2 \equiv -1 \pmod{p}. \tag{4.2}$$

Die multiplikative Gruppe des Körpers $\mathbb{Z}_p$ ist zyklisch. Sei $\alpha \in \mathbb{Z}$ so, dass $[\alpha]_p$ ein Erzeuger dieser Gruppe ist. Wir setzen $x := \alpha^{\frac{p-1}{4}}$ und erhalten aus dem Satz von Fermat $x^4 \equiv 1 \pmod{p}$. Es gilt also $p|(x^4-1)$, also $p|(x^2+1)(x-1)(x+1)$. Wenn $x \equiv 1 \pmod{p}$ oder $x \equiv -1 \pmod{p}$, so gilt $\alpha^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. Dann ist $[\alpha]_p$ kein Erzeuger von $\mathbb{Z}_p^*$. Folglich gilt $p|(x^2+1)$, und wir haben (4.2) bewiesen. (Eine andere Variante, die nicht verwendet, dass $\mathbb{Z}_p^*$ zyklisch ist, ist zu zeigen, dass $x := \frac{p-1}{2}!$ die Gleichung (4.2) erfüllt.) Nun wählen wir ein x, das die Gleichung (4.2) erfüllt. Im Ring $\mathbb{Z}[i]$ gilt natürlich ebenfalls $p|(1+x^2)$, also $p|(1+x\,i)\cdot(1-x\,i)$. Da jedes Vielfache von p im Ring $\mathbb{Z}[i]$ einen durch p teilbaren Realteil hat, gilt in $\mathbb{Z}[i]$ weder $p|(1+x\,i)$ noch $p|(1-x\,i)$. Im Ring $\mathbb{Z}[i]$ ist p also nicht prim. Da $\mathbb{Z}[i]$ als Hauptidealbereich auch faktoriell ist, ist jedes irreduzible Element von $\mathbb{Z}[i]$ prim. Somit ist p in $\mathbb{Z}[i]$ nicht irreduzibel. Es gibt also $a, b, c, d \in \mathbb{Z}$, sodass $p = (a+b\,i)(c+d\,i)$, und $a+b\,i$ und $c+d\,i$ nicht invertierbar sind. Es gilt

$$p^2 = N(p) = N((a+b\,i)(c+d\,i)) = N(a+b\,i)\cdot N(c+d\,i) = (a^2+b^2)(c^2+d^2).$$

Alle Elemente $z \in \mathbb{Z}[i]$ mit $N(z) = 1$ sind invertierbar. Somit muss $a^2+b^2 = p$ gelten. Die Zahlen $a' := |a|$ und $b' := |b|$ leisten also das Gewünschte. □

5. Teilbarkeit in Polynomringen

Definition 5.1. Sei R ein kommutativer Ring mit Eins, sei $n \in \mathbb{N}_0$, und sei $f = \sum_{i=0}^{n} f_i x^i \in R[x]$. Das Polynom f ist *primitiv*, wenn es kein primes $p \in R$ gibt, das alle Koeffizienten f_i $(i = 0, \ldots, n)$ teilt.

Lemma 5.2 (Gaußsches Lemma)**.** *Sei R ein kommutativer Ring mit Eins, und seien $f, g \in R[x]$ primitiv. Dann ist $f \cdot g$ ebenfalls primitiv.*

Beweis: Wir nehmen an, dass $f \cdot g$ nicht primitiv ist. Dann gibt es ein primes $p \in R$, das alle Koeffizienten von $f \cdot g$ teilt. Wir bezeichen mit $[f]_{(p)}$ das Polynom $\sum_{i=0}^{\deg f}(f_i+(p))x^i$ im Ring $R/(p)\,[x]$. Es gilt also dann $[f \cdot g]_{(p)} = 0$. Da (p) prim ist, ist $R/(p)$ ein Integritätsbereich. Daher ist auch $R/(p)[x]$ ein Integritätsbereich (der führende Koeffizient des Produkts zweier Polynome ist das Produkt der führenden Koeffizienten dieser zwei Polynome). Da $[f \cdot g]_{(p)} = [f]_{(p)} \cdot [g]_{(p)}$, muss also $[f]_{(p)}$ oder $[g]_{(p)}$ gleich 0 sein. Wenn $[f]_{(p)}$ gleich 0 ist, dann teilt p alle Koeffizienten von f, und f ist somit nicht primitiv; $[g]_{(p)} = 0$ bedeutet, dass g nicht primitiv ist. □

Lemma 5.3. *Sei R ein faktorieller Integritätsbereich, und sei $f \in R[x]$ mit $f \neq 0$. Dann gibt es $r \in R$, $g \in R[x]$, sodass g primitiv ist und $f = rg$.*

Beweis: Sei f_i ein Koeffizient von f, der $\neq 0$ ist. Sei $g \in R[x]$ so, dass das vom $i$ten Koeffizienten erzeugte Hauptideal (g_i) maximal in

$$\{(g_i') \,|\, g' \in R[x] \text{ und } \exists r \in R : rg' = f\}$$

ist, und sei $r \in R$ so, dass $rg = f$. Wenn g nicht primitiv ist, dann gibt es ein primes $p \in R$ und $h \in R[x]$, sodass $g = ph$. Für den $i$ten Koeffizienten gilt dann $g_i = ph_i$. Da $(g_i) \subseteq (h_i)$ und da $rp\,h = f$, gilt wegen der Maximalität von (g_i), dass $(g_i) = (h_i)$ ist. Also gibt es $s \in R$, sodass $s\,g_i = h_i$, und somit $sp\,h_i = h_i$. Da $h_i \neq 0$, ist p damit invertierbar, im Widerspruch dazu, dass p prim ist. Also ist g primitiv. □

Lemma 5.4. *Sei R ein faktorieller Integritätsbereich, und seien $g_1, g_2 \in R[x]$ primitive Polynome $\neq 0$, und seien $r_1, r_2 \in R$. Wenn $r_1 g_1 = r_2 g_2$, dann sind r_1 und r_2 in R assoziiert.*

Beweis: Wir fixieren $g_1, g_2 \in R[x] \setminus \{0\}$ und betrachten die Menge

$$A = \{(r_1, r_2) \in R \times R \,|\, r_1 g_1 = r_2 g_2 \text{ und } r_1 \not\sim_R r_2\}$$

Wenn diese Menge leer ist, dann ist der Satz bewiesen. Wenn die Menge nicht leer ist, dann wählen wir ein $(r_1, r_2) \in A$ so, dass (r_1) maximal in $\{(r_1') \,|\, (r_1', r_2') \in A\}$ ist. Da $g_1 \neq 0$, $g_2 \neq 0$ und R ein Integritätsbereich ist, gilt $r_1 \neq 0$.

Wenn r_1 invertierbar ist, dann ist $r_1 g_1$ primitiv. Wenn nun r_2 nicht invertierbar ist, dann gibt es ein primes $p \in R$, sodass $p | r_2$. Dann ist jeder Koeffizient von

r_2g_2 durch p teilbar, im Widerspruch dazu, dass r_1g_1 primitiv ist. Also ist r_2 invertierbar und damit zu r_1 assoziiert.

Wenn r_1 nicht invertierbar ist, so gibt es ein primes $p \in R \setminus \{0\}$, sodass $p|r_1$. Wegen $r_1g_1 = r_2g_2$ teilt p alle Koeffizienten von r_2g_2. Da p nicht alle Koeffizienten von g_2 teilt, muss es r_2 teilen. Es gibt also s_1, s_2, sodass $ps_1 = r_1$ und $ps_2 = r_2$. Es gilt $ps_1\, g_1 = ps_2\, g_2$. Wegen $p \neq 0$ gilt $s_1g_1 = s_2g_2$. Wenn $(r_1) = (s_1)$, so gibt es $t \in R$, sodass $tr_1 = s_1$, und somit $s_1 = tps_1$. Dann ist p invertierbar, ein Widerspruch. Somit gilt $(r_1) \subseteq (s_1)$ und $(r_1) \neq (s_1)$. Wegen der Maximalität von (r_1) sind s_1 und s_2 assoziiert, es gibt also ein invertierbares $u \in R$ mit $us_1 = s_2$. Dann gilt auch $ups_1 = ps_2$, also $ur_1 = r_2$. Dann sind auch r_1 und r_2 in R assoziiert, im Widerspruch zur Annahme, dass (r_1, r_2) in A liegt.

Die Menge A ist also leer; damit ist der Satz bewiesen. □

Satz 5.5. *Sei R ein faktorieller Integritätsbereich, und seien $f, g \in R[x] \setminus \{0\}$. Seien $r, s \in R$ und seien f_1, g_1 primitive Polynome in $R[x]$ so, dass $f = r\, f_1$ und $g = s\, g_1$. Sei $Q(R)$ der Quotientenkörper von R. Dann sind äquivalent:*

(1) *$f|g$ in $R[x]$.*
(2) *$f_1|g_1$ in $Q(R)[x]$ und $r|s$.*

Beweis: (1)⇒(2): Es gibt $h \in R[x]$, sodass $g = h \cdot f$. Wegen $g \neq 0$ gilt $s \neq 0$. Dann gilt $g_1 = s^{-1}\, g = s^{-1}\, (h \cdot f) = s^{-1} r\, (h \cdot f_1)$. Also gilt $f_1|g_1$ in $Q(R)[x]$. Außerdem gilt $h \cdot (r\, f_1) = s\, g_1$. Wir wählen $t \in R$ und $h_1 \in R[x]$ so, dass h_1 primitiv ist, und $t\, h_1 = h$. Es gilt dann $(t\, h_1) \cdot (r\, f_1) = s\, g_1$, also $rt\, (h_1 \cdot f_1) = s\, g_1$. Wegen des Gaußschen Lemmas ist $h_1 \cdot f_1$ primitiv. Somit sind wegen Lemma 5.4 die Elemente rt und s in R assoziiert. Damit gilt aber $r|s$.

(2)⇒(1): Wir wissen, dass es ein $h_1 \in Q(R)[x]$ gibt, sodass $f_1 \cdot h_1 = g_1$. Wir multiplizieren nun mit dem Produkt aller Nenner, die in den Koeffizienten von h_1 auftreten. Sei d dieses Produkt. Es gilt dann

$$f_1 \cdot (d\, h_1) = d\, g_1$$

und $d\, h_1 \in R[x]$. Sei nun $e \in R$ und sei h_2 ein primitives Polynom in $R[x]$ mit der Eigenschaft

$$e\, h_2 = d\, h_1.$$

Dann gilt

$$f_1 \cdot (e\, h_2) = d\, g_1,$$

also

$$e\, (f_1 \cdot h_2) = d\, g_1.$$

Wegen des Gaußschen Lemmas ist $f_1 \cdot h_2$ primitiv. Aus Lemma 5.4 erhalten wir, dass e und d assoziiert sind. Es gibt also ein invertierbares $u \in R$, sodass $e = du$. Somit gilt

$$du\, h_2 = d\, h_1.$$

Da $d \neq 0$, gilt $u\,h_2 = h_1$. Somit liegt h_1 in $R[x]$. Damit gilt $f_1|g_1$ auch in $R[x]$. Wegen $r|s$ gilt also auch $r\,f_1|s\,g_1$ in $R[x]$ und somit $f|g$. □

Lemma 5.6. *Sei R ein faktorieller Integritätsbereich, sei $Q(R)$ sein Quotientenkörper, und sei f ein primitives Polynom in $R[x] \setminus \{0\}$. Dann sind äquivalent:*

(1) *f ist ein irreduzibles Element von $R[x]$.*
(2) *f ist ein irreduzibles Element von $Q(R)[x]$.*

Beweis: (1)⇒(2): Wir nehmen an, dass f ein irreduzibles Element von $R[x]$ ist. Seien nun $g, h \in Q(R)[x]$ so, dass

$$f = g \cdot h.$$

Wir multiplizieren mit allen Nennern von g und h und erhalten $c, d \in R$, sodass

$$cd\,f = (c\,g) \cdot (d\,h),$$

$c, d \neq 0$, und $c\,g \in R[x]$, $d\,h \in R[x]$. Wir wählen $c_1, d_1 \in R$ und primitive Polynome $g_1, h_1 \in R[x]$ so, dass $c_1\,g_1 = c\,g$ und $d_1\,h_1 = d\,h$. Es gilt dann

$$cd\,f = c_1 d_1\,(g_1 \cdot h_1).$$

Wegen des Gaußschen Lemmas ist $g_1 \cdot h_1$ primitiv. Also sind cd und $c_1 d_1$ wegen Lemma 5.4 assoziiert. Es gibt also ein invertierbares Element $u \in R$, sodass

$$cd\,f = ucd\,(g_1 \cdot h_1).$$

Da R ein Integritätsbereich ist, gilt $cd \neq 0$ und somit

$$f = u\,(g_1 \cdot h_1).$$

Somit gilt $g_1|f$ und $h_1|f$ in $R[x]$. Da f irreduzibel in $R[x]$ ist, ist entweder g_1 oder h_1 invertierbar in $R[x]$, also vom Grad 0. Wenn g_1 Grad 0 hat, ist g in $Q(R)[x]$ invertierbar; wenn h_1 Grad 0 hat, ist h in $Q(R)[x]$ invertierbar. Damit ist f also irreduzibel in $Q(R)[x]$.

(2)⇒(1): Sei f ein primitives Polynom in $R[x] \setminus \{0\}$. Wir nehmen an, dass f irreduzibel in $Q(R)[x]$ ist. Seien nun $g, h \in R[x]$ so, dass $f = g \cdot h$. Da f irreduzibel in $Q(R)[x]$ ist, ist entweder g oder h invertierbar in $Q(R)[x]$, also ein konstantes Polynom $\neq 0$. Wir nehmen an, g ist konstant. Wenn der konstante Koeffizient von g nicht invertierbar ist, dann ist er durch ein primes Element p von R teilbar. Dann ist aber auch jeder Koeffizient von $f = g \cdot h$ durch p teilbar, im Widerspruch dazu, dass f primitiv ist. Folglich ist g ein konstantes Polynom in $R[x]$ mit einem in R invertierbaren konstanten Koeffizienten. Somit ist g in $R[x]$ invertierbar. Im Fall, dass h konstant ist, erhalten wir, dass h in $R[x]$ invertierbar ist. Insgesamt erhalten wir, dass f irreduzibel in $R[x]$ ist. □

Satz 5.7. *Sei R ein faktorieller Integritätsbereich. Dann ist auch $R[x]$ faktoriell.*

Beweis: Wir zeigen als erstes, dass $R[x]$ die ACC für Hauptideale erfüllt. Sei $a_1 \in R[x] \setminus \{0\}$, und sei $(a_1) \subseteq (a_2) \subseteq \cdots$ eine Folge von Hauptidealen. Für jedes $i \in \mathbb{N}$ wählen wir $r_i \in R$ und ein primitives $b_i \in R[x]$ so, dass $a_i = r_i\, b_i$. Wegen Satz 5.5 ist dann $(r_1)_R \subseteq (r_2)_R \subseteq \cdots$ eine aufsteigende Kette von Idealen in R und $(b_1)_{Q(R)[x]} \subseteq (b_2)_{Q(R)[x]} \subseteq \cdots$ eine aufsteigende Kette von Idealen in $Q(R)[x]$. R ist faktoriell, und erfüllt daher die ACC für Hauptideale. Der Ring $Q(R)[x]$ ist ein Polynomring über einem Körper. Als solcher ist er ein Hauptidealring (jedes Ideal I wird von jedem Polynom kleinsten Grades in $I \setminus \{0\}$ erzeugt), und somit faktoriell. Es gibt also ein $N \in \mathbb{N}$, sodass für alle $k \geq N$ gilt: $(r_N)_R = (r_k)_R$ und $(b_N)_{Q(R)[x]} = (b_k)_{Q(R)[x]}$. Es gilt also $b_N | b_k$ in $Q(R)[x]$ und $r_N | r_k$ in R. Somit gilt $a_N | a_k$ in $R[x]$, und somit $(a_k)_{R[x]} = (a_N)_{R[x]}$.

Nun zeigen wir, dass jedes irreduzible Element in $R[x]$ prim ist. Sei dazu $f \in R[x]$ irreduzibel, und seien $a, b \in R[x] \setminus \{0\}$ so, dass $f | a \cdot b$. Wir wollen nun zeigen, dass f in $R[x]$ entweder a oder b teilt.

Seien f_1, a_1, b_1 primitive Polynome in $R[x]$ und $r, s, t \in R$ so, dass $r\, f_1 = f$, $s\, a_1 = a$, $t\, b_1 = b$. Das Polynom f ist irreduzibel, also ist entweder r oder f_1 invertierbar in $R[x]$.

In dem Fall, dass f_1 invertierbar in $R[x]$ ist, ist ist f_1 ein Polynom vom Grad 0; sein konstanter und einziger Koeffizient ist ein invertierbares Element von R. Das Polynom f_1 ist also primitiv und es gilt nach Satz 5.5 $r | st$. Da f irreduzibel in $R[x]$ ist, ist r irreduzibel in R. R ist faktoriell, somit ist r prim, und es gilt $r | s$ oder $r | t$. Falls $r | s$, so gilt $r | sa_1$, und somit $r | a$ und damit $f | a$. Der Fall $r | t$ liefert analog $f | b$.

In dem Fall, dass f_1 nicht invertierbar in $R[x]$ ist, muss r invertierbar in $R[x]$, und damit in R, sein. Das Polynom f ist also primitiv, und folglich wegen Lemma 5.6 irreduzibel in $Q(R)[x]$. Da $f | a_1 b_1$ in $Q(R)[x]$ und f in $Q(R)[x]$ prim ist, gilt $f | a_1$ oder $f | b_1$ in $Q(R)[x]$. Wenn $f | a_1$ in $Q(R)[x]$, gilt nach Satz 5.5 auch $f | a_1$ in $R[x]$, und somit auch $f | a$. Wenn $f | b_1$ in $Q(R)[x]$, erhalten wir $f | b$.

Somit ist f prim. Nach Satz 3.5 ist $R[x]$ damit faktoriell. □

Korollar 5.8. *Sei R ein faktorieller Integritätsbereich und $k \in \mathbb{N}$. Dann ist $R[x_1, \ldots, x_k]$ faktoriell.*

6. Grösster gemeinsamer Teiler

Definition 6.1. Sei R ein Integritätsbereich, sei $n \in \mathbb{N}$, und seien $f_1, \ldots, f_n \in R$. Dann ist $d \in R$ ein *größter gemeinsamer Teiler* von $f_1, \ldots, f_n$, wenn

(1) $d | f_1, \ldots, d | f_n$.
(2) Für alle $d' \in R$ mit $d' | f_1, \ldots, d' | f_n$ gilt $d' | d$.

Satz 6.2. *Sei R ein faktorieller Ring, sei $n \in \mathbb{N}$, und seien $f_1, \ldots, f_n \in R$. Dann gibt es einen größten gemeinsamen Teiler von $f_1, \ldots, f_n$.*

Beweisskizze: Wir erhalten aus den Zerlegungen von $f_1, \ldots, f_n$ und Lemma 3.3 eine Zerlegung von d. □

Satz 6.3. *Sei R ein faktorieller Integritätsbereich, und seien $f_1, \ldots, f_n \in R[x] \setminus \{0\}$. Seien $r_1, \ldots, r_n \in R$ und $g_1, \ldots, g_n$ primitive Elemente in $R[x]$ so, dass $f_1 = r_1 g_1, \ldots, f_n = r_n g_n$.*

Es sei d_1 ein größter gemeinsamer Teiler von $r_1, \ldots, r_n$ in R, und d_2 ein größter gemeinsamer Teiler von $g_1, \ldots, g_n$ in $Q(R)[x]$. Wir nehmen an, dass d_2 primitiv in $R[x]$ ist.

Dann ist $d_1 d_2$ ein größter gemeinsamer Teiler von $f_1, \ldots, f_n$ in $R[x]$.

Beweis: Wir zeigen zunächst, dass $d_1 d_2$ alle f_i teilt. Sei $i \in \{1, \ldots, n\}$. Da $d_1 | r_i$ in R und $d_2 | g_i$ in $Q(R)[x]$, liefert Satz 5.5 auch $d_1 d_2 | f_i$ in $R[x]$.

Sei nun $d' \in R[x]$ so, dass d' in $R[x]$ alle f_i teilt. Wir wählen $d_1' \in R$ und ein primitives $d_2' \in R[x]$ so, dass $d' = d_1' d_2'$. Dann gilt wegen Satz 5.5, dass d_1' alle r_i in R teilt, und dass d_2' alle g_i in $Q(R)[x]$ teilt. Da d_1 ein größter gemeinsamer Teiler in R ist, gilt $d_1' | d_1$ in R. Da d_2 ein größter gemeinsamer Teiler in $Q(R)[x]$ ist, gilt $d_2' | d_2$ in $Q(R)[x]$. Wir verwenden wieder Satz 5.5 und erhalten $d_2' | d_2$ in $R[x]$. Somit gilt $d_1' d_2' | d_1 d_2$ in $R[x]$, und somit $d' | d$ in $R[x]$. □