HIR, faktorielle und euklidische Ringe

Thomas Markwig

keilen@mathematik.uni-kl.de

Universität Göttingen

HIR, faktorielle, euklidische Ringe

1.23 Definition

Es sei R ein IB, $r, r' \in R$.

HIR, faktorielle, euklidische Ringe

1.23 Definition

Es sei R ein IB, $r, r' \in R$.

$$r \mid r' \quad :\Longleftrightarrow \quad \exists\, t \in R \;:\; r' = r \cdot t$$

HIR, faktorielle, euklidische Ringe

1.23 Definition

Es sei R ein IB, $r, r' \in R$.

$$r \mid r' \quad :\Longleftrightarrow \quad \exists\, t \in R \,:\, r' = r \cdot t \quad \Longleftrightarrow \quad \langle r' \rangle \subseteq \langle r \rangle .$$

HIR, faktorielle, euklidische Ringe

1.23 Definition

Es sei R ein IB, $r, r' \in R$.

$$r \mid r' \quad :\Longleftrightarrow \quad \exists\, t \in R \,:\, r' = r \cdot t \quad \Longleftrightarrow \quad \langle r' \rangle \subseteq \langle r \rangle.$$

r assoziiert zu r' $\quad :\Longleftrightarrow \quad \exists\, u \in R^* \,:\, r = r' \cdot u$

HIR, faktorielle, euklidische Ringe

1.23 Definition

Es sei R ein IB, $r, r' \in R$.

$$r \mid r' \quad :\Longleftrightarrow \quad \exists\, t \in R \,:\, r' = r \cdot t \quad \Longleftrightarrow \quad \langle r' \rangle \subseteq \langle r \rangle.$$

r assoziiert zu r' $\quad :\Longleftrightarrow \quad \exists\, u \in R^* \,:\, r = r' \cdot u \quad \Longleftrightarrow \quad \langle r' \rangle = \langle r \rangle.$

HIR, faktorielle, euklidische Ringe

1.23 Definition

Es sei R ein IB, $r, r' \in R$.

$$r \mid r' \quad :\Longleftrightarrow \quad \exists\, t \in R \,:\, r' = r \cdot t \quad \Longleftrightarrow \quad \langle r' \rangle \subseteq \langle r \rangle.$$

r assoziiert zu r' $\quad :\Longleftrightarrow \quad \exists\, u \in R^* \,:\, r = r' \cdot u \quad \Longleftrightarrow \quad \langle r' \rangle = \langle r \rangle.$

$0 \neq r \in R \backslash R^*$ ist irreduzibel $\quad :\Longleftrightarrow \quad (r = s \cdot t \;\Rightarrow\; s \in R^* \text{ or } t \in R^*).$

HIR, faktorielle, euklidische Ringe

1.23 Definition

Es sei R ein IB, $r, r' \in R$.

$$r \mid r' \quad :\Longleftrightarrow \quad \exists\, t \in R \,:\, r' = r \cdot t \quad \Longleftrightarrow \quad \langle r' \rangle \subseteq \langle r \rangle.$$

r assoziiert zu r' $\quad :\Longleftrightarrow \quad \exists\, u \in R^* \,:\, r = r' \cdot u \quad \Longleftrightarrow \quad \langle r' \rangle = \langle r \rangle.$

$0 \neq r \in R \backslash R^*$ ist irreduzibel $\quad :\Longleftrightarrow \quad (r = s{\cdot}t \;\Rightarrow\; s \in R^* \text{ or } t \in R^*).$

$0 \neq r \in R \setminus R^*$ ist prim $\quad :\Longleftrightarrow \quad (r \mid s \cdot t \;\Rightarrow\; r \mid s \text{ oder } r \mid t)$

HIR, faktorielle, euklidische Ringe

1.23 Definition

Es sei R ein IB, $r, r' \in R$.

$$r \mid r' \quad :\Longleftrightarrow \quad \exists\, t \in R \,:\, r' = r \cdot t \quad \Longleftrightarrow \quad \langle r' \rangle \subseteq \langle r \rangle.$$

r assoziiert zu r' $\quad :\Longleftrightarrow \quad \exists\, u \in R^* \,:\, r = r' \cdot u \quad \Longleftrightarrow \quad \langle r' \rangle = \langle r \rangle.$

$0 \neq r \in R \backslash R^*$ ist irreduzibel $\quad :\Longleftrightarrow \quad (r = s \cdot t \;\Rightarrow\; s \in R^* \text{ or } t \in R^*).$

$0 \neq r \in R \setminus R^*$ ist prim $\quad :\Longleftrightarrow \quad (r \mid s \cdot t \;\Rightarrow\; r \mid s \text{ oder } r \mid t)$

$\Longleftrightarrow \quad \langle r \rangle$ ist ein Primideal.

HIR, faktorielle, euklidische Ringe

1.24 Beispiel

a. r prim $\Longrightarrow$ r irreduzibel.

HIR, faktorielle, euklidische Ringe

1.24 Beispiel

a. r prim $\Longrightarrow$ r irreduzibel.

b. r, s irreduzibel, $r \mid s$ $\Longrightarrow$ $\langle r \rangle = \langle s \rangle$.

HIR, faktorielle, euklidische Ringe

1.24 Beispiel

a. r prim $\Longrightarrow$ r irreduzibel.

b. r, s irreduzibel, $r \mid s$ $\Longrightarrow$ $\langle r \rangle = \langle s \rangle$.

c. $R = \mathbb{Z}$: p irreduzibel $\Leftrightarrow$ p prim $\Leftrightarrow$ p Primzahl.

HIR, faktorielle, euklidische Ringe

1.24 Beispiel

a. r prim $\Longrightarrow$ r irreduzibel.

b. r, s irreduzibel, $r \mid s$ $\Longrightarrow$ $\langle r \rangle = \langle s \rangle$.

c. $R = \mathbb{Z}$: p irreduzibel $\Leftrightarrow$ p prim $\Leftrightarrow$ p Primzahl.

d. $R = K[x]$: f irreduzibel $\Leftrightarrow$ f prim.

HIR, faktorielle, euklidische Ringe

1.24 Beispiel

a. r prim $\Longrightarrow$ r irreduzibel.

b. r, s irreduzibel, $r \mid s$ $\Longrightarrow$ $\langle r \rangle = \langle s \rangle$.

c. $R = \mathbb{Z}$: p irreduzibel $\Leftrightarrow$ p prim $\Leftrightarrow$ p Primzahl.

d. $R = K[x]$: f irreduzibel $\Leftrightarrow$ f prim.

e. $R = K[[x]]$: p irreduzibel $\Leftrightarrow$ p prim $\Leftrightarrow$ $p = Einheit \cdot x^{\mathrm{ord}(p)} = 1$.

HIR, faktorielle, euklidische Ringe

1.25 Definition

Es sei R ein IB.

a. R ist euklidisch $:\Longleftrightarrow$ $\exists\ \nu : R \setminus \{0\} \to \mathbb{N}$, so daß

HIR, faktorielle, euklidische Ringe

1.25 Definition

Es sei R ein IB.

a. R ist euklidisch $:\Longleftrightarrow$ $\exists\, \nu : R \setminus \{0\} \to \mathbb{N}$, so daß

$$\forall\, a, b \in R \setminus \{0\}\ \ \exists\, q, r \in R\ : a = q \cdot b + r$$

mit $r = 0$ oder $0 \leq \nu(r) < \nu(b)$.

HIR, faktorielle, euklidische Ringe

1.25 Definition

Es sei R ein IB.

a. R ist euklidisch $:\Longleftrightarrow$ $\exists\, \nu : R \setminus \{0\} \to \mathbb{N}$, so daß

$$\forall\, a, b \in R \setminus \{0\}\ \ \exists\, q, r \in R\ : a = q \cdot b + r$$

mit $r = 0$ oder $0 \leq \nu(r) < \nu(b)$.

Die Zerlegung heißt Division mit Rest (DmR).

HIR, faktorielle, euklidische Ringe

1.25 Definition

Es sei R ein IB.

a. R ist euklidisch $:\Longleftrightarrow$ $\exists\, \nu : R \setminus \{0\} \to \mathbb{N}$, so daß

$$\forall\, a, b \in R \setminus \{0\}\ \ \exists\, q, r \in R\ : a = q \cdot b + r$$

mit $r = 0$ oder $0 \leq \nu(r) < \nu(b)$.

Die Zerlegung heißt Division mit Rest (DmR).

b. R ist ein HIR (Hauptidealring) $:\Leftrightarrow$ alle Ideale sind Hauptideale.

HIR, faktorielle, euklidische Ringe

1.25 Definition

Es sei R ein IB.

a. R ist euklidisch $:\Longleftrightarrow$ $\exists\, \nu : R \setminus \{0\} \to \mathbb{N}$, so daß

$$\forall\, a, b \in R \setminus \{0\}\ \ \exists\, q, r \in R\ : a = q \cdot b + r$$

mit $r = 0$ oder $0 \leq \nu(r) < \nu(b)$.

Die Zerlegung heißt Division mit Rest (DmR).

b. R ist ein HIR (Hauptidealring) $:\Leftrightarrow$ alle Ideale sind Hauptideale.

c. R ist faktoriell (ZPE) $:\Longleftrightarrow$

$$(0 \neq r \in R \setminus R^* \implies \exists\, p_i \text{ prim } :\ r = p_1 \cdots p_k).$$

HIR, faktorielle, euklidische Ringe

1.26 Beispiel

a. $\mathbb{Z}$ ist euklidisch mit $\nu(z) = |z|$.

HIR, faktorielle, euklidische Ringe

1.26 Beispiel

a. $\mathbb{Z}$ ist euklidisch mit $\nu(z) = |z|$.

b. $K[x]$ ist euklidisch mit $\nu(f) = \deg(f)$.

HIR, faktorielle, euklidische Ringe

1.26 Beispiel

a. $\mathbb{Z}$ ist euklidisch mit $\nu(z) = |z|$.

b. $K[x]$ ist euklidisch mit $\nu(f) = \deg(f)$.

c. $K[[x]]$ ist euklidisch mit $\nu(f) = \mathrm{ord}(f)$.

HIR, faktorielle, euklidische Ringe

1.26 Beispiel

a. $\mathbb{Z}$ ist euklidisch mit $\nu(z) = |z|$.

b. $K[x]$ ist euklidisch mit $\nu(f) = \deg(f)$.

c. $K[[x]]$ ist euklidisch mit $\nu(f) = \mathrm{ord}(f)$.

d. $\mathbb{Z}[i] = \{x + iy \mid x, y \in \mathbb{Z}\} \leq \mathbb{C}$ ist euklidisch mit

$$\nu(x + iy) = |x + iy|^2 = x^2 + y^2,$$

der Ring der ganzen Gaußschen Zahlen.

HIR, faktorielle, euklidische Ringe

1.27 Proposition

Seien $f, g \in R[x], \quad f = \sum_{i=0}^{n} f_i x^i, \quad f_n \neq 0.$

HIR, faktorielle, euklidische Ringe

1.27 Proposition

Seien $f, g \in R[x], \quad f = \sum_{i=0}^{n} f_i x^i, \quad f_n \neq 0.$

a. $\exists$

HIR, faktorielle, euklidische Ringe

1.27 Proposition

Seien $f, g \in R[x], \quad f = \sum_{i=0}^{n} f_i x^i, \quad f_n \neq 0.$

a. $\exists\, k \geq 0,\ q, r \in R[x]$, *so daß*

$$f_n^k \cdot g = q \cdot f + r \quad \textit{und} \quad \deg(r) < \deg(f).$$

HIR, faktorielle, euklidische Ringe

1.27 Proposition

Seien $f, g \in R[x], \quad f = \sum_{i=0}^{n} f_i x^i, \quad f_n \neq 0.$

a. $\exists\ k \geq 0,\ q, r \in R[x]$, *so daß*

$$f_n^k \cdot g = q \cdot f + r \quad \textit{und} \quad \deg(r) < \deg(f).$$

b. R *IB* , $\quad f_n \in R^* \quad \Longrightarrow \quad \exists!\, q, r \in R\ :\ g = q \cdot f + r.$

HIR, faktorielle, euklidische Ringe

1.28 Theorem

$$R \quad \textit{euklidisch} \quad \Longrightarrow \quad R \quad \textit{HIR}.$$

HIR, faktorielle, euklidische Ringe

1.28 Theorem

$$R \quad \textit{euklidisch} \quad \Longrightarrow \quad R \quad \textit{HIR}.$$

Beweis:

Imitiere den Beweis für $\mathbb{Z}$, “minimal” durch “minimal bez. ν”. $\square$

HIR, faktorielle, euklidische Ringe

1.28 Theorem

$$R \quad \textit{euklidisch} \quad \Longrightarrow \quad R \quad \textit{HIR}.$$

Beweis:

Imitiere den Beweis für $\mathbb{Z}$, “minimal” durch “minimal bez. ν”. □

1.29 Korollar $\mathbb{Z}$, $\mathbb{Z}[i]$, $K[x]$, $K[[x]]$, $\mathbb{R}\{x\}$ und $\mathbb{C}\{x\}$ sind HIR.

HIR, faktorielle, euklidische Ringe

1.28 Theorem

$$R \quad \textit{euklidisch} \quad \Longrightarrow \quad R \quad \textit{HIR}.$$

Beweis:

Imitiere den Beweis für $\mathbb{Z}$, “minimal” durch “minimal bez. ν”. $\square$

1.29 Korollar $\mathbb{Z}$, $\mathbb{Z}[i]$, $K[x]$, $K[[x]]$, $\mathbb{R}\{x\}$ und $\mathbb{C}\{x\}$ sind HIR.

1.30 Proposition Sei R ein HIR, $r \in R$.

HIR, faktorielle, euklidische Ringe

1.28 Theorem

$$R \quad \textit{euklidisch} \quad \Longrightarrow \quad R \quad \textit{HIR}.$$

Beweis:

Imitiere den Beweis für $\mathbb{Z}$, “minimal” durch “minimal bez. ν”. $\square$

1.29 Korollar $\mathbb{Z}$, $\mathbb{Z}[i]$, $K[x]$, $K[[x]]$, $\mathbb{R}\{x\}$ und $\mathbb{C}\{x\}$ sind HIR.

1.30 Proposition Sei R ein HIR, $r \in R$.

a. r irreduzibel $\quad \Longleftrightarrow \quad \langle r \rangle \lhd \cdot R$.

HIR, faktorielle, euklidische Ringe

1.28 Theorem

$$R \quad \textit{euklidisch} \quad \Longrightarrow \quad R \quad \textit{HIR}.$$

Beweis:

Imitiere den Beweis für $\mathbb{Z}$, "minimal" durch "minimal bez. ν". $\square$

1.29 Korollar $\mathbb{Z}$, $\mathbb{Z}[i]$, $K[x]$, $K[[x]]$, $\mathbb{R}\{x\}$ und $\mathbb{C}\{x\}$ sind HIR.

1.30 Proposition Sei R ein HIR, $r \in R$.

a. r irreduzibel $\quad \Longleftrightarrow \quad \langle r \rangle \lhd \cdot R$.

b. r irreduzibel $\quad \Longrightarrow \quad r$ prim.

HIR, faktorielle, euklidische Ringe

1.28 Theorem

$$R \quad \textit{euklidisch} \quad \Longrightarrow \quad R \quad \textit{HIR}.$$

Beweis:

Imitiere den Beweis für $\mathbb{Z}$, "minimal" durch "minimal bez. ν". $\square$

1.29 Korollar $\mathbb{Z}$, $\mathbb{Z}[i]$, $K[x]$, $K[[x]]$, $\mathbb{R}\{x\}$ und $\mathbb{C}\{x\}$ sind HIR.

1.30 Proposition Sei R ein HIR, $r \in R$.

a. r irreduzibel $\Longleftrightarrow$ $\langle r \rangle \lhd \cdot R$.

b. r irreduzibel $\Longrightarrow$ r prim.

c. $\mathrm{Spec}(R) = \mathfrak{m} - \mathrm{Spec}(R) \cup \{\langle 0 \rangle\}$

HIR, faktorielle, euklidische Ringe

1.31 Beispiel

$3 \in \mathbb{Z}[\sqrt{-5}] = \{x + y \cdot \sqrt{-5} \mid x, y \in \mathbb{Z}\}$ ist irred., nicht prim.

HIR, faktorielle, euklidische Ringe

1.31 Beispiel

$3 \in \mathbb{Z}\left[\sqrt{-5}\right] = \left\{x + y \cdot \sqrt{-5} \;\middle|\; x, y \in \mathbb{Z}\right\}$ ist irred., nicht prim.

Insbesondere, $\mathbb{Z}\left[\sqrt{-5}\right]$ ist kein HIR.

HIR, faktorielle, euklidische Ringe

1.31 Beispiel

$3 \in \mathbb{Z}\left[\sqrt{-5}\right] = \left\{x + y \cdot \sqrt{-5} \;\middle|\; x, y \in \mathbb{Z}\right\}$ ist irred., nicht prim.

Insbesondere, $\mathbb{Z}\left[\sqrt{-5}\right]$ ist kein HIR.

1.32 Korollar

$$R \quad \textit{HIR} \quad \Longrightarrow \quad R \quad \textit{faktoriell.}$$

HIR, faktorielle, euklidische Ringe

1.31 Beispiel

$3 \in \mathbb{Z}\left[\sqrt{-5}\right] = \left\{x + y \cdot \sqrt{-5} \;\middle|\; x, y \in \mathbb{Z}\right\}$ ist irred., nicht prim.

Insbesondere, $\mathbb{Z}\left[\sqrt{-5}\right]$ ist kein HIR.

1.32 Korollar

$$R \quad \textit{HIR} \quad \Longrightarrow \quad R \quad \textit{faktoriell.}$$

1.33 Korollar $\mathbb{Z}$, $\mathbb{Z}[i]$, $K[x]$, $K[[x]]$, $\mathbb{R}\{x\}$, $\mathbb{C}\{x\}$ sind faktoriell.

HIR, faktorielle, euklidische Ringe

1.34 Proposition Die folgenden Aussagen sind gleichwertig:

HIR, faktorielle, euklidische Ringe

1.34 Proposition Die folgenden Aussagen sind gleichwertig:

a. R ist faktoriell.

HIR, faktorielle, euklidische Ringe

1.34 Proposition Die folgenden Aussagen sind gleichwertig:

a. R ist faktoriell.

b. (r irreduzibel $\Longrightarrow$ r prim)

HIR, faktorielle, euklidische Ringe

1.34 Proposition Die folgenden Aussagen sind gleichwertig:

a. R ist faktoriell.

b. (r irreduzibel $\Longrightarrow$ r prim) und

$(0 \neq r \in R \setminus R^* \quad \Longrightarrow \quad \exists\, p_i \text{ irreduzibel} \;:\; r = p_1 \cdots p_k)$.

HIR, faktorielle, euklidische Ringe

1.34 Proposition Die folgenden Aussagen sind gleichwertig:

a. R ist faktoriell.

b. (r irreduzibel $\Longrightarrow$ r prim) und

$(0 \neq r \in R \setminus R^* \quad \Longrightarrow \quad \exists\, p_i$ irreduzibel $: \; r = p_1 \cdots p_k)$.

c. $(0 \neq r \in R \setminus R^* \quad \Rightarrow \quad \exists\, p_i$ irreduzibel $: \; r = p_1 \cdots p_k)$.

HIR, faktorielle, euklidische Ringe

1.34 Proposition Die folgenden Aussagen sind gleichwertig:

a. R ist faktoriell.

b. (r irreduzibel $\Longrightarrow$ r prim) und

$(0 \neq r \in R \setminus R^* \Longrightarrow \exists\, p_i$ irreduzibel $: r = p_1 \cdots p_k)$.

c. $(0 \neq r \in R \setminus R^* \Rightarrow \exists$ eind. irred. $p_i : r = p_1 \cdots p_k)$.

HIR, faktorielle, euklidische Ringe

1.34 Proposition Die folgenden Aussagen sind gleichwertig:

a. R ist faktoriell.

b. (r irreduzibel $\implies$ r prim) und

$(0 \neq r \in R \setminus R^* \implies \exists\, p_i \text{ irreduzibel} : r = p_1 \cdots p_k)$.

c. $(0 \neq r \in R \setminus R^* \Rightarrow \exists$ eind. irred. $p_i : r = p_1 \cdots p_k)$.
d.h. wenn $r = p_1 \cdots p_k = q_1 \cdots q_l$ mit p_i, q_i irred., dann

- $k = l$, und
- nach Umordnung $\langle p_i \rangle = \langle q_i \rangle$ für alle i.

HIR, faktorielle, euklidische Ringe

1.35 Definition Sei R faktoriell und $r_1, \ldots, r_k \in R$.

HIR, faktorielle, euklidische Ringe

1.35 Definition Sei R faktoriell und $r_1, \ldots, r_k \in R$.

a. g ist ein ggT (größter gemeins. Teiler) von $r_1, \ldots, r_k$

$$:\Longleftrightarrow \quad g \mid r_i \; \forall \; i \quad \text{und} \quad (t \mid r_i \; \forall \; i \implies t \mid g)$$

HIR, faktorielle, euklidische Ringe

1.35 Definition Sei R faktoriell und $r_1, \ldots, r_k \in R$.

a. g ist ein ggT (größter gemeins. Teiler) von $r_1, \ldots, r_k$

$$:\Longleftrightarrow \quad g \mid r_i \ \forall\, i \quad \text{und} \quad (t \mid r_i \ \forall\, i \implies t \mid g)$$

$$\Longleftrightarrow \quad g \mid r_i \ \forall\, i \quad \text{und} \quad \nexists\, p \text{ irred.} : p \mid \frac{r_i}{g} \ \forall\, i$$

HIR, faktorielle, euklidische Ringe

1.35 Definition Sei R faktoriell und $r_1, \ldots, r_k \in R$.

a. g ist ein ggT (größter gemeins. Teiler) von $r_1, \ldots, r_k$

$$:\Longleftrightarrow \quad g \mid r_i \; \forall \, i \quad \text{und} \quad (t \mid r_i \; \forall \, i \implies t \mid g)$$

Not.: $\mathrm{ggT}(r_1, \ldots, r_k) = \{g \in R \mid g \text{ ist ggT von } r_1, \ldots, r_k\}$.

HIR, faktorielle, euklidische Ringe

1.35 Definition Sei R faktoriell und $r_1, \ldots, r_k \in R$.

a. g ist ein ggT (größter gemeins. Teiler) von $r_1, \ldots, r_k$

$$:\Longleftrightarrow \quad g \mid r_i \; \forall \; i \quad \text{und} \quad (t \mid r_i \; \forall \; i \implies t \mid g)$$

Not.: $\mathrm{ggT}(r_1, \ldots, r_k) = \{g \in R \mid g \text{ ist ggT von } r_1, \ldots, r_k\}$.

b. l ist kgV (kleinstes gemeins. Vielfaches) von $r_1, \ldots, r_k$

$$:\Longleftrightarrow \quad r_i \mid l \; \forall \; i \quad \text{und} \quad (r_i \mid t \; \forall \; i \implies l \mid t)$$

HIR, faktorielle, euklidische Ringe

1.35 Definition Sei R faktoriell und $r_1, \ldots, r_k \in R$.

a. g ist ein ggT (größter gemeins. Teiler) von $r_1, \ldots, r_k$

$$:\Longleftrightarrow \quad g \mid r_i \; \forall \; i \quad \text{und} \quad (t \mid r_i \; \forall \; i \implies t \mid g)$$

Not.: $\mathrm{ggT}(r_1, \ldots, r_k) = \{g \in R \mid g \text{ ist ggT von } r_1, \ldots, r_k\}$.

b. l ist kgV (kleinstes gemeins. Vielfaches) von $r_1, \ldots, r_k$

$$:\Longleftrightarrow \quad r_i \mid l \; \forall \; i \quad \text{und} \quad (r_i \mid t \; \forall \; i \implies l \mid t)$$

$$\overset{k=2}{\Longleftrightarrow} \quad r_1, r_2 \mid l \quad \text{und} \quad \frac{r_1 \cdot r_2}{l} \in \mathrm{ggT}(r_1, r_2).$$

HIR, faktorielle, euklidische Ringe

1.35 Definition Sei R faktoriell und $r_1, \ldots, r_k \in R$.

a. g ist ein ggT (größter gemeins. Teiler) von $r_1, \ldots, r_k$

$$:\Longleftrightarrow \quad g \mid r_i \; \forall \; i \quad \text{und} \quad (t \mid r_i \; \forall \; i \implies t \mid g)$$

Not.: $\mathrm{ggT}(r_1, \ldots, r_k) = \{g \in R \mid g \text{ ist ggT von } r_1, \ldots, r_k\}$.

b. l ist kgV (kleinstes gemeins. Vielfaches) von $r_1, \ldots, r_k$

$$:\Longleftrightarrow \quad r_i \mid l \; \forall \; i \quad \text{und} \quad (r_i \mid t \; \forall \; i \implies l \mid t)$$

Not.: $\mathrm{kgV}(r_1, \ldots, r_k) = \{l \in R \mid l \text{ ist kgV von } r_1, \ldots, r_k\}$.

HIR, faktorielle, euklidische Ringe

1.36 Bemerkung Sei R ein HIR.

HIR, faktorielle, euklidische Ringe

1.36 Bemerkung Sei R ein HIR.

$$g \in \mathrm{ggT}(r_1, \ldots, r_k) \quad \Longleftrightarrow \quad \langle g \rangle = \langle r_1, \ldots, r_k \rangle$$

HIR, faktorielle, euklidische Ringe

1.36 Bemerkung Sei R ein HIR.

$$g \in \mathrm{ggT}(r_1, \ldots, r_k) \iff \langle g \rangle = \langle r_1, \ldots, r_k \rangle$$

und

$$l \in \mathrm{kgV}(r_1, \ldots, r_k) \iff \langle l \rangle = \langle r_1 \rangle \cap \ldots \cap \langle r_k \rangle.$$

HIR, faktorielle, euklidische Ringe

1.36 Bemerkung Sei R ein HIR.

$$g \in \mathrm{ggT}(r_1, \ldots, r_k) \iff \langle g \rangle = \langle r_1, \ldots, r_k \rangle$$

und

$$l \in \mathrm{kgV}(r_1, \ldots, r_k) \iff \langle l \rangle = \langle r_1 \rangle \cap \ldots \cap \langle r_k \rangle.$$

1.37 Lemma Sei R ein IB und $r \in R$.

HIR, faktorielle, euklidische Ringe

1.36 Bemerkung Sei R ein HIR.

$$g \in \mathrm{ggT}(r_1, \ldots, r_k) \iff \langle g \rangle = \langle r_1, \ldots, r_k \rangle$$

und

$$l \in \mathrm{kgV}(r_1, \ldots, r_k) \iff \langle l \rangle = \langle r_1 \rangle \cap \ldots \cap \langle r_k \rangle.$$

1.37 Lemma Sei R ein IB und $r \in R$.

a. $R[x]^* = R^*$.

HIR, faktorielle, euklidische Ringe

1.36 Bemerkung Sei R ein HIR.

$$g \in \mathrm{ggT}(r_1, \ldots, r_k) \iff \langle g \rangle = \langle r_1, \ldots, r_k \rangle$$

und

$$l \in \mathrm{kgV}(r_1, \ldots, r_k) \iff \langle l \rangle = \langle r_1 \rangle \cap \ldots \cap \langle r_k \rangle.$$

1.37 Lemma Sei R ein IB und $r \in R$.

a. $R[x]^* = R^*$.

b. r irreduzibel in R $\implies$ r irreduzibel in $R[x]$.

HIR, faktorielle, euklidische Ringe

1.36 Bemerkung Sei R ein HIR.

$$g \in \mathrm{ggT}(r_1, \ldots, r_k) \iff \langle g \rangle = \langle r_1, \ldots, r_k \rangle$$

und

$$l \in \mathrm{kgV}(r_1, \ldots, r_k) \iff \langle l \rangle = \langle r_1 \rangle \cap \ldots \cap \langle r_k \rangle.$$

1.37 Lemma Sei R ein IB und $r \in R$.

a. $R[x]^* = R^*$.

b. r irreduzibel in $R \implies r$ irreduzibel in $R[x]$.

c. r prim in $R \implies r$ prim in $R[x]$.

HIR, faktorielle, euklidische Ringe

1.38 Theorem (Lemma von Gauß)

$$R \text{ ist } \textit{faktoriell} \quad \Longrightarrow \quad R[x] \text{ ist } \textit{faktoriell}.$$

HIR, faktorielle, euklidische Ringe

1.38 Theorem (Lemma von Gauß)

$$R \text{ ist } \textit{faktoriell} \implies R[x] \text{ ist } \textit{faktoriell}.$$

1.39 Korollar K ein Körper $\implies$ $K[x_1, \ldots, x_n]$ ein faktoriell.

HIR, faktorielle, euklidische Ringe

1.38 Theorem (Lemma von Gauß)

$$R \text{ ist } \textit{faktoriell} \implies R[x] \text{ ist } \textit{faktoriell}.$$

1.39 Korollar K ein Körper $\implies$ $K[x_1, \ldots, x_n]$ ein faktoriell.

1.40 Korollar $R[x]$ ist ein HIR $\iff$ R ist ein Körper.

HIR, faktorielle, euklidische Ringe

1.38 Theorem (Lemma von Gauß)

$$R \text{ ist } \textit{faktoriell} \iff R[x] \text{ ist } \textit{faktoriell}.$$

1.39 Korollar K ein Körper $\iff$ $K[x_1, \ldots, x_n]$ ein faktoriell.

1.40 Korollar $R[x]$ ist ein HIR $\iff$ R ist ein Körper.

Insbesondere, $K[x_1, \ldots, x_n]$ ist kein HIR für $n \geq 2$.

HIR, faktorielle, euklidische Ringe

1.38 Theorem (Lemma von Gauß)

$$R \text{ ist } \textit{faktoriell} \iff R[x] \text{ ist } \textit{faktoriell}.$$

1.39 Korollar K ein Körper $\iff$ $K[x_1, \ldots, x_n]$ ein faktoriell.

1.40 Korollar $R[x]$ ist ein HIR $\iff$ R ist ein Körper.

Insbesondere, $K[x_1, \ldots, x_n]$ ist kein HIR für $n \geq 2$.

1.41 Theorem

$$\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right] \textit{ ist ein HIR, aber nicht euklidisch.}$$

HIR, faktorielle, euklidische Ringe

1.46 Bemerkung

Aus Theorem 1.41, Korollar 1.39 und 1.40 wissen wir:

$$R \text{ ist euklidisch} \implies R \text{ ist ein HIR} \implies R \text{ ist faktoriell},$$

aber

$$R \text{ ist euklidisch} \not\Longleftarrow R \text{ ist ein HIR} \not\Longleftarrow R \text{ ist faktoriell}.$$

HIR, faktorielle, euklidische Ringe

1.42 Proposition Sei R ein IB.

R ist ein HIR $\iff$ $\exists\, \alpha : R \to \mathbb{N}$, so daß

HIR, faktorielle, euklidische Ringe

1.42 Proposition Sei R ein IB.

R ist ein HIR $\iff$ $\exists\, \alpha : R \to \mathbb{N}$, so daß

$$\forall\, 0 \neq b \nmid a \quad \exists\, u, v \in R \;:\; \alpha(0) < \alpha(ua - vb) < \alpha(b).$$

HIR, faktorielle, euklidische Ringe

1.42 Proposition Sei R ein IB.

R ist ein HIR $\iff$ $\exists\, \alpha : R \to \mathbb{N}$, so daß

$$\forall\, 0 \neq b \nmid a \quad \exists\, u, v \in R \;:\; \alpha(0) < \alpha(ua - vb) < \alpha(b).$$

Idee: $g = ua - vb \in \mathrm{ggT}(a, b)$ und $\langle g \rangle = \langle a, b \rangle$!

HIR, faktorielle, euklidische Ringe

1.42 Proposition Sei R ein IB.

R ist ein HIR $\iff$ $\exists\, \alpha : R \to \mathbb{N}$, so daß

$$\forall\, 0 \neq b \nmid a \quad \exists\, u, v \in R \;:\; \alpha(0) < \alpha(ua - vb) < \alpha(b).$$

Idee: $g = ua - vb \in \mathrm{ggT}(a, b)$ und $\langle g \rangle = \langle a, b \rangle$!

1.43 Proposition R euklidisch, $0 \neq p \in R \setminus R^*$ minimal bez. ν, $\pi : R \to R/\langle p \rangle : a \mapsto \overline{a}$. Dann:

HIR, faktorielle, euklidische Ringe

1.42 Proposition Sei R ein IB.

R ist ein HIR $\iff$ $\exists\, \alpha : R \to \mathbb{N}$, so daß

$$\forall\, 0 \neq b \nmid a \quad \exists\, u, v \in R \;:\; \alpha(0) < \alpha(ua - vb) < \alpha(b).$$

Idee: $g = ua - vb \in \mathrm{ggT}(a, b)$ und $\langle g \rangle = \langle a, b \rangle$!

1.43 Proposition R euklidisch, $0 \neq p \in R \setminus R^*$ minimal bez. ν, $\pi : R \to R/\langle p \rangle : a \mapsto \overline{a}$. Dann:

a. p ist prim & $K = R/\langle p \rangle$ ist ein Körper.

HIR, faktorielle, euklidische Ringe

1.42 Proposition Sei R ein IB.

R ist ein HIR $\iff$ $\exists\, \alpha : R \to \mathbb{N}$, so daß

$$\forall\, 0 \neq b \nmid a \quad \exists\, u, v \in R \;:\; \alpha(0) < \alpha(ua - vb) < \alpha(b).$$

Idee: $g = ua - vb \in \mathrm{ggT}(a, b)$ und $\langle g \rangle = \langle a, b \rangle$!

1.43 Proposition R euklidisch, $0 \neq p \in R \setminus R^*$ minimal bez. ν, $\pi : R \to R/\langle p \rangle : a \mapsto \overline{a}$. Dann:

a. p ist prim & $K = R/\langle p \rangle$ ist ein Körper.

b. $a \in R \implies a = q \cdot p + r$ mit $r = 0$ or $r \in R^*$.

HIR, faktorielle, euklidische Ringe

1.42 Proposition Sei R ein IB.

R ist ein HIR $\iff$ $\exists\, \alpha : R \to \mathbb{N}$, so daß

$$\forall\, 0 \neq b \nmid a \quad \exists\, u, v \in R \;:\; \alpha(0) < \alpha(ua - vb) < \alpha(b).$$

Idee: $g = ua - vb \in \mathrm{ggT}(a, b)$ und $\langle g \rangle = \langle a, b \rangle$!

1.43 Proposition R euklidisch, $0 \neq p \in R \setminus R^*$ minimal bez. ν, $\pi : R \to R/\langle p \rangle : a \mapsto \overline{a}$. Dann:

a. p ist prim & $K = R/\langle p \rangle$ ist ein Körper.

b. $a \in R \implies a = q \cdot p + r$ mit $r = 0$ or $r \in R^*$.

c. $\pi(R^*) = K^*$.

HIR, faktorielle, euklidische Ringe

Beweis von Theorem 1.41, see [Bru00]:

Definiere eine *Norm* $N : R \to \mathbb{N}$ auf $R = \mathbb{Z}[\omega]$, $\omega = \frac{1+\sqrt{-19}}{2}$:

$$N(a + b\omega) = |a + b\omega|^2$$

HIR, faktorielle, euklidische Ringe

Beweis von Theorem 1.41, see [Bru00]:

Definiere eine *Norm* $N : R \to \mathbb{N}$ auf $R = \mathbb{Z}[\omega]$, $\omega = \frac{1+\sqrt{-19}}{2}$:

$$N(a+b\omega) = |a+b\omega|^2 = \left(a+\frac{b}{2}\right)^2 + 19 \cdot \frac{b^2}{4}$$

HIR, faktorielle, euklidische Ringe

Beweis von Theorem 1.41, see [Bru00]:

Definiere eine *Norm* $N : R \to \mathbb{N}$ auf $R = \mathbb{Z}[\omega]$, $\omega = \frac{1+\sqrt{-19}}{2}$:

$$N(a+b\omega) = |a+b\omega|^2 = \left(a+\frac{b}{2}\right)^2 + 19 \cdot \frac{b^2}{4} = a^2 + ab + 5b^2 \in \mathbb{N}.$$

HIR, faktorielle, euklidische Ringe

Beweis von Theorem 1.41, see [Bru00]:

Definiere eine *Norm* $N : R \to \mathbb{N}$ auf $R = \mathbb{Z}[\omega]$, $\omega = \frac{1+\sqrt{-19}}{2}$:

$$N(a+b\omega) = |a+b\omega|^2 = \left(a+\frac{b}{2}\right)^2 + 19 \cdot \frac{b^2}{4} = a^2 + ab + 5b^2 \in \mathbb{N}.$$

Beh.: $R^* = \{1, -1\} = \{x \in R \mid N(x) = 1\}$.

HIR, faktorielle, euklidische Ringe

Beweis von Theorem 1.41, see [Bru00]:

Definiere eine *Norm* $N : R \to \mathbb{N}$ auf $R = \mathbb{Z}[\omega]$, $\omega = \frac{1+\sqrt{-19}}{2}$:

$$N(a+b\omega) = |a+b\omega|^2 = \left(a+\frac{b}{2}\right)^2 + 19 \cdot \frac{b^2}{4} = a^2 + ab + 5b^2 \in \mathbb{N}.$$

Beh.: $R^* = \{1, -1\} = \{x \in R \mid N(x) = 1\}$.

$$1 = x \cdot y \quad \Longrightarrow \quad 1 = |x|^2 \cdot |y|^2 \quad \text{mit} \quad |x|^2, |y|^2 \in \mathbb{N}.$$

HIR, faktorielle, euklidische Ringe

Beweis von Theorem 1.41, see [Bru00]:

Definiere eine *Norm* $N : R \to \mathbb{N}$ auf $R = \mathbb{Z}[\omega]$, $\omega = \frac{1+\sqrt{-19}}{2}$:

$$N(a+b\omega) = |a+b\omega|^2 = \left(a+\frac{b}{2}\right)^2 + 19 \cdot \frac{b^2}{4} = a^2 + ab + 5b^2 \in \mathbb{N}.$$

Beh.: $R^* = \{1, -1\} = \{x \in R \mid N(x) = 1\}$.

$$1 = x \cdot y \quad \Longrightarrow \quad 1 = |x|^2 \cdot |y|^2 \quad \text{mit} \quad |x|^2, |y|^2 \in \mathbb{N}.$$

Damit:

$$1 = |x|^2 = N(x) = \left(a+\frac{b}{2}\right)^2 + 19 \cdot \frac{b^2}{4}.$$

HIR, faktorielle, euklidische Ringe

Beweis von Theorem 1.41, see [Bru00]:

Definiere eine *Norm* $N : R \to \mathbb{N}$ auf $R = \mathbb{Z}[\omega]$, $\omega = \frac{1+\sqrt{-19}}{2}$:

$$N(a+b\omega) = |a+b\omega|^2 = \left(a+\frac{b}{2}\right)^2 + 19 \cdot \frac{b^2}{4} = a^2 + ab + 5b^2 \in \mathbb{N}.$$

Beh.: $R^* = \{1, -1\} = \{x \in R \mid N(x) = 1\}$.

$$1 = x \cdot y \quad \Longrightarrow \quad 1 = |x|^2 \cdot |y|^2 \quad \text{mit} \quad |x|^2, |y|^2 \in \mathbb{N}.$$

Außerdem, wenn $x = a + b \cdot \omega$:

$$b^2 = 0, \left(a+\frac{b}{2}\right)^2 = 1 \quad \Longrightarrow \quad b = 0, a \in \{1, -1\}.$$

HIR, faktorielle, euklidische Ringe

Beh.: 2 und 3 sind irreduzibel.

$$2 = x \cdot y, \qquad \Longrightarrow \qquad 4 = |x|^2 \cdot |y|^2 = N(x) \cdot N(y),$$

HIR, faktorielle, euklidische Ringe

Beh.: 2 und 3 sind irreduzibel.

$$2 = x \cdot y, \;\; x, y \notin R^* \quad \Longrightarrow \quad 4 = |x|^2 \cdot |y|^2 = N(x) \cdot N(y),$$

mit $N(x), N(y) > 1$

HIR, faktorielle, euklidische Ringe

Beh.: 2 und 3 sind irreduzibel.

$$2 = x \cdot y, \;\; x, y \notin R^* \quad \Longrightarrow \quad 4 = |x|^2 \cdot |y|^2 = N(x) \cdot N(y),$$

mit $N(x), N(y) > 1$

$$\Longrightarrow \quad 2 = N(x)$$

HIR, faktorielle, euklidische Ringe

Beh.: 2 und 3 sind irreduzibel.

$$2 = x \cdot y, \;\; x, y \notin R^* \quad \Longrightarrow \quad 4 = |x|^2 \cdot |y|^2 = N(x) \cdot N(y),$$

mit $N(x), N(y) > 1$

$$\Longrightarrow \quad 2 = N(x) = N(a + b \cdot \omega) = \left(a + \frac{b}{2}\right)^2 + \frac{19}{4} \cdot b^2.$$

HIR, faktorielle, euklidische Ringe

Beh.: 2 und 3 sind irreduzibel.

$$2 = x \cdot y, \;\; x, y \notin R^* \quad \Longrightarrow \quad 4 = |x|^2 \cdot |y|^2 = N(x) \cdot N(y),$$

mit $N(x), N(y) > 1$

$$\Longrightarrow \quad 2 = N(x) = N(a + b \cdot \omega) = \left(a + \frac{b}{2}\right)^2 + \frac{19}{4} \cdot b^2.$$

$$\Longrightarrow \quad b = 0$$

HIR, faktorielle, euklidische Ringe

Beh.: 2 und 3 sind irreduzibel.

$$2 = x \cdot y, \;\; x, y \notin R^* \quad \Longrightarrow \quad 4 = |x|^2 \cdot |y|^2 = N(x) \cdot N(y),$$

mit $N(x), N(y) > 1$

$$\Longrightarrow \quad 2 = N(x) = N(a + b \cdot \omega) = \left(a + \frac{b}{2}\right)^2 + \frac{19}{4} \cdot b^2.$$

$$\Longrightarrow \quad b = 0 \quad \Longrightarrow \quad a^2 = 2 \quad , \quad a \in \mathbb{Z} \quad \lightning\lightning\lightning$$

HIR, faktorielle, euklidische Ringe

Beh.: 2 und 3 sind irreduzibel.

$$2 = x \cdot y, \;\; x, y \notin R^* \quad \Longrightarrow \quad 4 = |x|^2 \cdot |y|^2 = N(x) \cdot N(y),$$

mit $N(x), N(y) > 1$

$$\Longrightarrow \quad 2 = N(x) = N(a + b \cdot \omega) = \left(a + \frac{b}{2}\right)^2 + \frac{19}{4} \cdot b^2.$$

$$\Longrightarrow \quad b = 0 \quad \Longrightarrow \quad a^2 = 2 \quad , \quad a \in \mathbb{Z} \quad \lightning\lightning\lightning$$

Der Beweis für 3 geht analog.

HIR, faktorielle, euklidische Ringe

Beh.: R ist nicht euklidisch.

HIR, faktorielle, euklidische Ringe

Beh.: R ist nicht euklidisch.

Ang., R wäre euklidisch und wähle $p \in R$ wie in 1.43.

HIR, faktorielle, euklidische Ringe

Beh.: R ist nicht euklidisch.

Ang., R wäre euklidisch und wähle $p \in R$ wie in 1.43.

D.h. $0 \neq p \in R$ minimal bez. ν und dann

- p ist prim.
- $K = R/\langle p \rangle$ ist Körper.
- $a \in R \implies a = q \cdot p + r$ mit $r = 0$ oder $r \in R^*$.
- $|K^*| \leq |R^*|$.

HIR, faktorielle, euklidische Ringe

Beh.: R ist nicht euklidisch.

Ang., R wäre euklidisch und wähle $p \in R$ wie in 1.43.

$$\Longrightarrow \quad |R/\langle p \rangle| = |K| \leq |R^*| + 1 = 3.$$

HIR, faktorielle, euklidische Ringe

Beh.: R ist nicht euklidisch.

Ang., R wäre euklidisch und wähle $p \in R$ wie in 1.43.

$$\Longrightarrow \quad |R/\langle p\rangle| = |K| \leq |R^*| + 1 = 3.$$

Beachte:

$$|R/\langle 2\rangle| = \left|\left\{\overline{0}, \overline{1}, \overline{\sqrt{-19}}, \overline{1+\sqrt{-19}}\right\}\right| = 4$$

und

$$|R/\langle 3\rangle| = \left|\left\{\overline{0}, \overline{1}, \overline{2}, \overline{\sqrt{-19}}, \overline{1+\sqrt{-19}}, \overline{2+\sqrt{-19}}\right\}\right| = 6.$$

HIR, faktorielle, euklidische Ringe

Beh.: R ist nicht euklidisch.

Ang., R wäre euklidisch und wähle $p \in R$ wie in 1.43.

$$\Longrightarrow \quad |R/\langle p \rangle| = |K| \leq |R^*| + 1 = 3.$$

Also:

$$\langle 2 \rangle \neq \langle p \rangle \neq \langle 3 \rangle.$$

HIR, faktorielle, euklidische Ringe

Beh.: R ist nicht euklidisch.

Ang., R wäre euklidisch und wähle $p \in R$ wie in 1.43.

$$\Longrightarrow \quad |R/\langle p\rangle| = |K| \leq |R^*| + 1 = 3.$$

Also:

$$\langle 2\rangle \neq \langle p\rangle \neq \langle 3\rangle.$$

Insbesondere:

$2 = q \cdot p + r$ mit $r \neq 0$

HIR, faktorielle, euklidische Ringe

Beh.: R ist nicht euklidisch.

Ang., R wäre euklidisch und wähle $p \in R$ wie in 1.43.

$$\Longrightarrow \quad |R/\langle p\rangle| = |K| \leq |R^*| + 1 = 3.$$

Also:

$$\langle 2\rangle \neq \langle p\rangle \neq \langle 3\rangle.$$

Insbesondere:

$$2 = q \cdot p + r \quad \text{mit } r \neq 0 \quad \Longrightarrow \quad r \in R^* = \{1, -1\}.$$

HIR, faktorielle, euklidische Ringe

Beh.: R ist nicht euklidisch.

Ang., R wäre euklidisch und wähle $p \in R$ wie in 1.43.

$$\Longrightarrow \quad |R/\langle p\rangle| = |K| \leq |R^*| + 1 = 3.$$

Also:

$$\langle 2\rangle \neq \langle p\rangle \neq \langle 3\rangle.$$

Insbesondere:

$$2 = q \cdot p + r \quad \text{mit } r \neq 0 \quad \Longrightarrow \quad r \in R^* = \{1, -1\}.$$

$$\Longrightarrow \quad \begin{cases} q \cdot p = 1 & \text{↯↯↯ zu } p \text{ prim,} \end{cases}$$

HIR, faktorielle, euklidische Ringe

Beh.: R ist nicht euklidisch.

Ang., R wäre euklidisch und wähle $p \in R$ wie in 1.43.

$$\Longrightarrow \quad |R/\langle p\rangle| = |K| \leq |R^*| + 1 = 3.$$

Also:

$$\langle 2\rangle \neq \langle p\rangle \neq \langle 3\rangle.$$

Insbesondere:

$$2 = q \cdot p + r \quad \text{mit } r \neq 0 \quad \Longrightarrow \quad r \in R^* = \{1, -1\}.$$

$$\Longrightarrow \begin{cases} q \cdot p = 1 & \text{↯↯↯ zu } p \text{ prim,} \\ q \cdot p = 3 \;\Rightarrow\; p \mid 3 & \text{↯↯↯ zu } 3 \text{ irred. } \langle p\rangle \neq \langle 3\rangle. \end{cases}$$

HIR, faktorielle, euklidische Ringe

Beh.:

$$\forall\, x, y \in R \;:\; 0 \neq y \not| x \quad \exists\, u, v \in R \;:\; 0 < \left| u \cdot \frac{x}{y} - v \right|^2 < 1.$$

HIR, faktorielle, euklidische Ringe

Beh.:

$$\forall\, x, y \in R \;:\; 0 \neq y \nmid x \quad \exists\, u, v \in R \;:\; 0 < \left| u \cdot \frac{x}{y} - v \right|^2 < 1.$$

Beachte:

$$\frac{x}{y} \in \mathbb{Q}[\omega] \quad \Longrightarrow \quad \exists\, a', b', a, b, q, s \in \mathbb{Z} \text{ mit } 0 \leq a < q, 0 \leq b < s,$$

$$1 \in \mathrm{ggT}(a, q) \text{ und } 1 \in \mathrm{ggT}(b, s),$$

$$\text{so daß } \frac{x}{y} = \left(a' + \frac{a}{q}\right) + \left(b' + \frac{b}{s}\right) \cdot \omega.$$

HIR, faktorielle, euklidische Ringe

Ziel: $0 < \left| u \cdot \frac{x}{y} - v \right|^2 < 1$ wobei $\frac{x}{y} = \left(a' + \frac{a}{q}\right) + \left(b' + \frac{b}{s}\right) \cdot \omega.$

HIR, faktorielle, euklidische Ringe

Ziel: $0 < \left| u \cdot \frac{x}{y} - v \right|^2 < 1$ wobei $\frac{x}{y} = \left(a' + \frac{a}{q}\right) + \left(b' + \frac{b}{s}\right) \cdot \omega.$

Wenn $u', v' \in R$, so daß

$$0 < \left| u' \cdot \left(\frac{a}{q} + \frac{b}{s} \cdot \omega \right) - v' \right| < 1,$$

HIR, faktorielle, euklidische Ringe

Ziel: $0 < \left| u \cdot \frac{x}{y} - v \right|^2 < 1$ wobei $\frac{x}{y} = \left(a' + \frac{a}{q}\right) + \left(b' + \frac{b}{s}\right) \cdot \omega.$

Wenn $u', v' \in R$, so daß

$$0 < \left| u' \cdot \left(\frac{a}{q} + \frac{b}{s} \cdot \omega \right) - v' \right| < 1,$$

dann tun es $u = u'$ und $v = v' + u' \cdot (a' + b' \cdot \omega)$, da

$$u \cdot \frac{x}{y} - v = u' \cdot \left(\frac{a}{q} + \frac{b}{s} \cdot \omega \right) + u' \cdot (a' + b' \cdot \omega) - v' - u' \cdot (a' + b' \cdot \omega)$$

HIR, faktorielle, euklidische Ringe

Ziel: $0 < \left| u \cdot \frac{x}{y} - v \right|^2 < 1$ wobei $\frac{x}{y} = \left(a' + \frac{a}{q}\right) + \left(b' + \frac{b}{s}\right) \cdot \omega.$

Wenn $u', v' \in R$, so daß

$$0 < \left| u' \cdot \left(\frac{a}{q} + \frac{b}{s} \cdot \omega \right) - v' \right| < 1,$$

dann tun es $u = u'$ und $v = v' + u' \cdot (a' + b' \cdot \omega)$, da

$$u \cdot \frac{x}{y} - v = u' \cdot \left(\frac{a}{q} + \frac{b}{s} \cdot \omega \right) - v'.$$

HIR, faktorielle, euklidische Ringe

Ziel: $0 < \left| u \cdot \frac{x}{y} - v \right|^2 < 1$ wobei $\frac{x}{y} = \left(a' + \frac{a}{q}\right) + \left(b' + \frac{b}{s}\right) \cdot \omega.$

Wenn $u', v' \in R$, so daß

$$0 < \left| u' \cdot \left(\frac{a}{q} + \frac{b}{s} \cdot \omega \right) - v' \right| < 1,$$

dann tun es $u = u'$ und $v = v' + u' \cdot (a' + b' \cdot \omega)$, da

$$u \cdot \frac{x}{y} - v = u' \cdot \left(\frac{a}{q} + \frac{b}{s} \cdot \omega \right) - v'.$$

Wir können deshalb $a' = b' = 0$ annehmen.

HIR, faktorielle, euklidische Ringe

Ziel: $0 < \left| u \cdot \frac{x}{y} - v \right|^2 < 1$ wobei $\frac{x}{y} = \frac{a}{q} + \frac{b}{s} \cdot \omega$ und

- $0 \leq a < q$,
- $0 \leq b < s$,
- $1 \in \mathrm{ggT}(a, q)$, und
- $1 \in \mathrm{ggT}(b, s)$.

HIR, faktorielle, euklidische Ringe

Ziel: $0 < \left| u \cdot \frac{x}{y} - v \right|^2 < 1$ wobei $\frac{x}{y} = \frac{a}{q} + \frac{b}{s} \cdot \omega$

1. Fall $b = 0$: Dann tun es $u = 1$ und $v = 0$.

HIR, faktorielle, euklidische Ringe

Ziel: $0 < \left| u \cdot \frac{x}{y} - v \right|^2 < 1$ wobei $\frac{x}{y} = \frac{a}{q} + \frac{b}{s} \cdot \omega$

1. Fall $b = 0$: Dann tun es $u = 1$ und $v = 0$.

2. Fall $b \neq 0$, $q \nmid s$: Dann

$$q \nmid s \cdot a \Longrightarrow \quad \exists\, 0<d<q,\ c \in \mathbb{Z} \ :\ sa = cq + d,$$

HIR, faktorielle, euklidische Ringe

Ziel: $0 < \left| u \cdot \frac{x}{y} - v \right|^2 < 1$ wobei $\frac{x}{y} = \frac{a}{q} + \frac{b}{s} \cdot \omega$

1. Fall $b = 0$: Dann tun es $u = 1$ und $v = 0$.

2. Fall $b \neq 0$, $q \nmid s$: Dann

$$q \nmid s \cdot a \Longrightarrow \quad \exists\, 0<d<q,\ c \in \mathbb{Z} \ :\ sa = cq + d,$$

und $u = s$ und $v = c + b\omega$ tun es:

$$\left| s \cdot \frac{x}{y} - (c + b\omega) \right|^2 = \left| \frac{sa}{q} + b\omega - c - b\omega \right|^2 = \left| \frac{d}{q} \right|^2.$$

HIR, faktorielle, euklidische Ringe

Ziel: $0 < \left| u \cdot \frac{x}{y} - v \right|^2 < 1$ wobei $\frac{x}{y} = \frac{a}{q} + \frac{b}{s} \cdot \omega$.

1. Fall $b = 0$: Dann $u = 1$ und $v = 0$ tun es.

2. Fall $b \neq 0$, $q \nmid s$: Dann $u = s$ und $v = c + b\omega$ tun es.

3. Fall $b \neq 0$, $q \mid s$, $s > 2$:

HIR, faktorielle, euklidische Ringe

Ziel: $0 < \left| u \cdot \frac{x}{y} - v \right|^2 < 1$ wobei $\frac{x}{y} = \frac{a}{q} + \frac{b}{s} \cdot \omega$.

3. Fall $b \neq 0, \quad q \mid s, \quad s > 2$: Dann

$$1 \in \mathrm{ggT}(s, b) \implies \exists\, m \in \mathbb{Z} \ : \ m \cdot b \equiv 1 \ (\mathrm{mod}\ s)$$

HIR, faktorielle, euklidische Ringe

Ziel: $0 < \left| u \cdot \frac{x}{y} - v \right|^2 < 1$ wobei $\frac{x}{y} = \frac{a}{q} + \frac{b}{s} \cdot \omega$.

3. Fall $b \neq 0, \quad q \mid s, \quad s > 2$: Dann

$$1 \in \mathrm{ggT}(s, b) \implies \exists\, m \in \mathbb{Z} \;:\; m \cdot b \equiv 1 \pmod{s}$$

$$\implies \frac{ma}{q} + \frac{mb}{s} \cdot \omega = \left(l + \frac{a_1}{a_2} \right) + \left(k + \frac{1}{s} \right) \cdot \omega$$

für geeignete $l, k, a_1, a_2 \in \mathbb{Z}$ mit $\left| \frac{a_1}{a_2} \right| \leq \frac{1}{2}$.

HIR, faktorielle, euklidische Ringe

Ziel: $0 < \left| u \cdot \frac{x}{y} - v \right|^2 < 1$ wobei $\frac{x}{y} = \frac{a}{q} + \frac{b}{s} \cdot \omega$.

3. Fall $b \neq 0, \quad q \mid s, \quad s > 2$:

$$\frac{ma}{q} + \frac{mb}{s} \cdot \omega = \left(l + \frac{a_1}{a_2} \right) + \left(k + \frac{1}{s} \right) \cdot \omega \text{ mit } \left| \frac{a_1}{a_2} \right| \leq \frac{1}{2}.$$

Dann tun es $u = m$ und $v = l + k\omega$:

$$\left| u \cdot \frac{x}{y} - v \right|^2 = \left| \frac{a_1}{a_2} + \frac{1}{s} \cdot \frac{1 + \sqrt{-19}}{2} \right|^2$$

HIR, faktorielle, euklidische Ringe

Ziel: $0 < \left| u \cdot \frac{x}{y} - v \right|^2 < 1$ wobei $\frac{x}{y} = \frac{a}{q} + \frac{b}{s} \cdot \omega$.

3. Fall $b \neq 0, \quad q \mid s, \quad s > 2$:

$$\frac{ma}{q} + \frac{mb}{s} \cdot \omega = \left(l + \frac{a_1}{a_2} \right) + \left(k + \frac{1}{s} \right) \cdot \omega \text{ mit } \left| \frac{a_1}{a_2} \right| \leq \frac{1}{2}.$$

Dann tun es $u = m$ und $v = l + k\omega$:

$$\left| u \cdot \frac{x}{y} - v \right|^2 = \left| \frac{a_1}{a_2} + \frac{1}{s} \cdot \frac{1 + \sqrt{-19}}{2} \right|^2 = \left(\frac{a_1}{a_2} + \frac{1}{2s} \right)^2 + \frac{19}{4s^2}$$

HIR, faktorielle, euklidische Ringe

Ziel: $0 < \left| u \cdot \frac{x}{y} - v \right|^2 < 1$ wobei $\frac{x}{y} = \frac{a}{q} + \frac{b}{s} \cdot \omega$.

3. Fall $b \neq 0, \quad q \mid s, \quad s > 2$:

$$\frac{ma}{q} + \frac{mb}{s} \cdot \omega = \left(l + \frac{a_1}{a_2} \right) + \left(k + \frac{1}{s} \right) \cdot \omega \text{ mit } \left| \frac{a_1}{a_2} \right| \leq \frac{1}{2}.$$

Dann tun es $u = m$ und $v = l + k\omega$:

$$\left| u \cdot \frac{x}{y} - v \right|^2 = \left| \frac{a_1}{a_2} + \frac{1}{s} \cdot \frac{1 + \sqrt{-19}}{2} \right|^2 = \left(\frac{a_1}{a_2} + \frac{1}{2s} \right)^2 + \frac{19}{4s^2}$$

$$= \frac{a_1^2}{a_2^2} + \frac{a_1}{a_2 s} + \frac{20}{4s^2}$$

HIR, faktorielle, euklidische Ringe

Ziel: $0 < \left| u \cdot \frac{x}{y} - v \right|^2 < 1$ wobei $\frac{x}{y} = \frac{a}{q} + \frac{b}{s} \cdot \omega$.

3. Fall $b \neq 0, \quad q \mid s, \quad s > 2$:

$$\frac{ma}{q} + \frac{mb}{s} \cdot \omega = \left(l + \frac{a_1}{a_2} \right) + \left(k + \frac{1}{s} \right) \cdot \omega \text{ mit } \left| \frac{a_1}{a_2} \right| \leq \frac{1}{2}.$$

Dann tun es $u = m$ und $v = l + k\omega$:

$$0 \neq \left| u \cdot \frac{x}{y} - v \right|^2 = \left| \frac{a_1}{a_2} + \frac{1}{s} \cdot \frac{1 + \sqrt{-19}}{2} \right|^2 = \left(\frac{a_1}{a_2} + \frac{1}{2s} \right)^2 + \frac{19}{4s^2}$$

$$= \frac{a_1^2}{a_2^2} + \frac{a_1}{a_2 s} + \frac{20}{4s^2} \leq \frac{1}{4} + \frac{1}{6} + \frac{20}{36} = \frac{35}{36} < 1.$$

HIR, faktorielle, euklidische Ringe

Ziel: $0 < \left| u \cdot \frac{x}{y} - v \right|^2 < 1$ wobei $\frac{x}{y} = \frac{a}{q} + \frac{b}{s} \cdot \omega$.

1. Fall $b = 0$: Dann $u = 1$ und $v = 0$ tun es.

2. Fall $b \neq 0$, $q \nmid s$: Dann $u = s$ und $v = c + b\omega$ tun es.

3. Fall $b \neq 0$, $q \mid s$, $s > 2$: Dann $u = m$, $v = l + k\omega$ tun es.

4. Fall $b \neq 0$, $q \mid s$, $s = 2$:

HIR, faktorielle, euklidische Ringe

Ziel: $0 < \left| u \cdot \frac{x}{y} - v \right|^2 < 1$ wobei $\frac{x}{y} = \frac{a}{q} + \frac{b}{s} \cdot \omega$.

4. Fall $b \neq 0, \quad q \mid s, \quad s = 2$: Dann tun es $q = s = 2$

$$\Longrightarrow \left\{ \begin{array}{lll} \frac{x}{y} = \frac{\omega}{2} & \Longrightarrow & u = 1 + \omega, v = -2 + \omega \\ \frac{x}{y} = \frac{1+\omega}{2} & \Longrightarrow & u = \omega, \quad v = -2 + \omega \end{array} \right\} \text{ da:}$$

HIR, faktorielle, euklidische Ringe

Ziel: $0 < \left| u \cdot \frac{x}{y} - v \right|^2 < 1$ wobei $\frac{x}{y} = \frac{a}{q} + \frac{b}{s} \cdot \omega$.

4. Fall $b \neq 0, \quad q \mid s, \quad s = 2$: Dann tun es $q = s = 2$

$$\Longrightarrow \left\{ \begin{array}{lll} \frac{x}{y} = \frac{\omega}{2} & \Longrightarrow & u = 1 + \omega, v = -2 + \omega \\ \frac{x}{y} = \frac{1+\omega}{2} & \Longrightarrow & u = \omega, \quad v = -2 + \omega \end{array} \right\} \text{ da:}$$

$$0 \neq \left| u \cdot \frac{x}{y} - v \right|^2 = \left| -\frac{1}{2} \right|^2 = \frac{1}{4} < 1,$$

HIR, faktorielle, euklidische Ringe

Damit ist die Behauptung bewiesen:

$$\forall\, x, y \in R \;:\; 0 \neq y \not| x \quad \exists\, u, v \in R \;:\; 0 < \left| u \cdot \frac{x}{y} - v \right|^2 < 1$$

HIR, faktorielle, euklidische Ringe

Damit ist die Behauptung bewiesen:

$$\forall\, x, y \in R \;:\; 0 \neq y \not| x \quad \exists\, u, v \in R \;:\; 0 < \left| u \cdot \frac{x}{y} - v \right|^2 < 1$$

und

Proposition 1.42 mit $\alpha = N \quad \Longrightarrow \quad R$ ist ein HIR!

□

HIR, faktorielle, euklidische Ringe

1.45 Bemerkung

a. $|K : \mathbb{Q}| = 2 \iff K = \mathbb{Q}[\sqrt{d}], 0, 1 \neq d \in \mathbb{Z}$ quadratfrei.

HIR, faktorielle, euklidische Ringe

1.45 Bemerkung

a. $|K : \mathbb{Q}| = 2 \iff K = \mathbb{Q}[\sqrt{d}], 0, 1 \neq d \in \mathbb{Z}$ quadratfrei.

b. $\mathbb{Z}[\omega_d] = \{a \in \mathbb{Q}[\sqrt{d}] \mid a \text{ ganz}\}$ für

$$\omega_d = \begin{cases} \sqrt{d}, & d \equiv 2, 3 \pmod 4 \\ \frac{1+\sqrt{d}}{2}, & d \equiv 1 \pmod 4. \end{cases}$$

HIR, faktorielle, euklidische Ringe

1.45 Bemerkung

a. $|K : \mathbb{Q}| = 2 \iff K = \mathbb{Q}\left[\sqrt{d}\right], 0, 1 \neq d \in \mathbb{Z}$ quadratfrei.

b. $\mathbb{Z}[\omega_d] = \left\{a \in \mathbb{Q}\left[\sqrt{d}\right] \mid a \text{ ganz}\right\}$

c. $\mathbb{Z}[\omega_d]$ ist faktoriell $\iff$ $\mathbb{Z}[\omega_d]$ ist ein HIR.

HIR, faktorielle, euklidische Ringe

1.45 Bemerkung

a. $|K : \mathbb{Q}| = 2 \iff K = \mathbb{Q}\left[\sqrt{d}\right], 0, 1 \neq d \in \mathbb{Z}$ quadratfrei.

b. $\mathbb{Z}[\omega_d] = \left\{a \in \mathbb{Q}\left[\sqrt{d}\right] \mid a \text{ ganz}\right\}$

c. $\mathbb{Z}[\omega_d]$ ist faktoriell $\iff$ $\mathbb{Z}[\omega_d]$ ist ein HIR.

d. Wenn $d \leq -1$ dann

HIR, faktorielle, euklidische Ringe

1.45 Bemerkung

a. $|K : \mathbb{Q}| = 2 \iff K = \mathbb{Q}[\sqrt{d}], 0, 1 \neq d \in \mathbb{Z}$ quadratfrei.

b. $\mathbb{Z}[\omega_d] = \{a \in \mathbb{Q}[\sqrt{d}] \mid a \text{ ganz}\}$

c. $\mathbb{Z}[\omega_d]$ ist faktoriell $\iff$ $\mathbb{Z}[\omega_d]$ ist ein HIR.

d. Wenn $d \leq -1$ dann

$\mathbb{Z}[\omega_d]$ faktoriell $\Leftrightarrow$ $d \in \{-1, -2, -3, -7, -11, -19, -43, -67, -163\}$,

HIR, faktorielle, euklidische Ringe

1.45 Bemerkung

a. $|K : \mathbb{Q}| = 2 \iff K = \mathbb{Q}[\sqrt{d}], 0, 1 \neq d \in \mathbb{Z}$ quadratfrei.

b. $\mathbb{Z}[\omega_d] = \{a \in \mathbb{Q}[\sqrt{d}] \mid a \text{ ganz}\}$

c. $\mathbb{Z}[\omega_d]$ ist faktoriell $\iff$ $\mathbb{Z}[\omega_d]$ ist ein HIR.

d. Wenn $d \leq -1$ dann

$$\mathbb{Z}[\omega_d] \text{ faktoriell} \Leftrightarrow d \in \{-1, -2, -3, -7, -11, -19, -43, -67, -163\},$$

und

$$\mathbb{Z}[\omega_d] \text{ ist euklidisch} \iff d \in \{-1, -2, -3, -7, -11\}.$$

HIR, faktorielle, euklidische Ringe

Literatur

[AtM69] Michael F. Atiyah and Ian G. MacDonald, *Introduction to commutative algebra*, Addison-Wesley, 1969.

[Bru00] Winfried Bruns, *Zahlentheorie*, OSM, Reihe V, no. 146, FB Mathematik/Informatik, Universität Osnabrück, 2000.

[ScS88] Günter Scheja and Uwe Storch, *Lehrbuch der Algebra*, Mathematische Leitfäden, vol. II, Teubner, 1988.