PID's, UFD's and Euclidean Rings

Thomas Markwig

keilen@mathematik.uni-kl.de

Technical University of Kaiserslautern

PID’s, UFD’s and Euclidean Rings

1.23 Definition

Let R be an ID, $r, r' \in R$.

PID's, UFD's and Euclidean Rings

1.23 Definition

Let R be an ID, $r, r' \in R$.

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

PID's, UFD's and Euclidean Rings

1.23 Definition

Let R be an ID, $r, r' \in R$.

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

PID's, UFD's and Euclidean Rings

1.23 Definition

Let R be an ID, $r, r' \in R$.

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

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

PID's, UFD's and Euclidean Rings

1.23 Definition

Let R be an ID, $r, r' \in R$.

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

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

PID's, UFD's and Euclidean Rings

1.23 Definition

Let R be an ID, $r, r' \in R$.

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

r associated to r' $\quad :\Longleftrightarrow \quad \exists\, u \in R^* \;:\; r = r' \cdot u \quad \Longleftrightarrow \quad \langle r' \rangle = \langle r \rangle.$

$0 \neq r \in R \setminus R^*$ is irreducible $\quad :\Longleftrightarrow \quad \big(r = s \cdot t \;\Rightarrow\; s \in R^*$ or $t \in R^*\big).$

PID's, UFD's and Euclidean Rings

1.23 Definition

Let R be an ID, $r, r' \in R$.

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

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

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

$0 \neq r \in R \setminus R^*$ is prime $\quad :\Longleftrightarrow \quad \left(r \mid s \cdot t \;\Rightarrow\; r \mid s \text{ or } r \mid t \right)$

PID's, UFD's and Euclidean Rings

1.23 Definition

Let R be an ID, $r, r' \in R$.

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

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

$0 \neq r \in R \backslash R^*$ is irreducible $\quad :\Longleftrightarrow \quad (r = s \cdot t \;\Rightarrow\; s \in R^*$ or $t \in R^*).$

$0 \neq r \in R \setminus R^*$ is prime $\quad :\Longleftrightarrow \quad (r \mid s \cdot t \;\Rightarrow\; r \mid s$ or $r \mid t)$

$\Longleftrightarrow \quad \langle r \rangle$ is a prime ideal.

PID's, UFD's and Euclidean Rings

1.24 Example

a. r prime $\Longrightarrow$ r irreducible.

PID's, UFD's and Euclidean Rings

1.24 Example

a. r prime $\Longrightarrow$ r irreducible.

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

PID's, UFD's and Euclidean Rings

1.24 Example

a. r prime $\Longrightarrow$ r irreducible.

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

c. $R = \mathbb{Z}$: p irreducible $\Leftrightarrow$ p prime $\Leftrightarrow$ p prime number.

PID's, UFD's and Euclidean Rings

1.24 Example

a. r prime $\Longrightarrow$ r irreducible.

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

c. $R = \mathbb{Z}$: p irreducible $\Leftrightarrow$ p prime $\Leftrightarrow$ p prime number.

d. $R = K[x]$: f irreducible $\Leftrightarrow$ f prime.

PID's, UFD's and Euclidean Rings

1.24 Example

a. r prime $\Longrightarrow$ r irreducible.

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

c. $R = \mathbb{Z}$: p irreducible $\Leftrightarrow$ p prime $\Leftrightarrow$ p prime number.

d. $R = K[x]$: f irreducible $\Leftrightarrow$ f prime.

e. $R = K[[x]]$: p irreducible $\Leftrightarrow$ p prime $\Leftrightarrow$ $p = unit \cdot x$

$\Leftrightarrow$ $\operatorname{ord}(p) = 1$.

PID's, UFD's and Euclidean Rings

1.25 Definition

Let R be an ID.

a. R is Euclidean $:\Longleftrightarrow \quad \exists\, \nu : R \setminus \{0\} \to \mathbb{N}$ such that

PID's, UFD's and Euclidean Rings

1.25 Definition

Let R be an ID.

a. R is Euclidean $:\Longleftrightarrow$ $\exists\, \nu : R\setminus\{0\} \to \mathbb{N}$ such that

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

with $r = 0$ or $0 \leq \nu(r) < \nu(b)$.

PID's, UFD's and Euclidean Rings

1.25 Definition

Let R be an ID.

a. R is Euclidean $:\Longleftrightarrow$ $\exists\, \nu : R \setminus \{0\} \to \mathbb{N}$ such that

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

with $r = 0$ or $0 \leq \nu(r) < \nu(b)$.

Call this decomposition a division with remainder (DwR).

PID's, UFD's and Euclidean Rings

1.25 Definition

Let R be an ID.

a. R is Euclidean $:\Longleftrightarrow$ $\exists\, \nu : R \setminus \{0\} \to \mathbb{N}$ such that

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

with $r = 0$ or $0 \leq \nu(r) < \nu(b)$.

Call this decomposition a division with remainder (DwR).

b. R is a PID (principle ideal domain) $:\Leftrightarrow$ all ideals are principle.

PID's, UFD's and Euclidean Rings

1.25 Definition

Let R be an ID.

a. R is Euclidean $:\Longleftrightarrow$ $\exists\,\nu : R\setminus\{0\}\to\mathbb{N}$ such that

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

with $r=0$ or $0\le\nu(r)<\nu(b)$.

Call this decomposition a division with remainder (DwR).

b. R is a PID (principle ideal domain) $:\Leftrightarrow$ all ideals are principle.

c. R is a UFD (unique factorisation domain) $:\Longleftrightarrow$

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

PID's, UFD's and Euclidean Rings

1.26 Example

a. $\mathbb{Z}$ is Euclidean with $\nu(z) = |z|$.

PID's, UFD's and Euclidean Rings

1.26 Example

a. $\mathbb{Z}$ is Euclidean with $\nu(z) = |z|$.

b. $K[x]$ is Euclidean with $\nu(f) = \deg(f)$.

PID's, UFD's and Euclidean Rings

1.26 Example

a. $\mathbb{Z}$ is Euclidean with $\nu(z) = |z|$.

b. $K[x]$ is Euclidean with $\nu(f) = \deg(f)$.

c. $K[[x]]$ is Euclidean with $\nu(f) = \mathrm{ord}(f)$.

PID's, UFD's and Euclidean Rings

1.26 Example

a. $\mathbb{Z}$ is Euclidean with $\nu(z) = |z|$.

b. $K[x]$ is Euclidean with $\nu(f) = \deg(f)$.

c. $K[[x]]$ is Euclidean with $\nu(f) = \operatorname{ord}(f)$.

d. $\mathbb{Z}[i] = \{x + iy \mid x, y \in \mathbb{Z}\} \leq \mathbb{C}$ is Euclidean with

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

it is called the Ring of Gaussian Integers.

PID's, UFD's and Euclidean Rings

1.27 Proposition

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

PID's, UFD's and Euclidean Rings

1.27 Proposition

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

a. $\exists$

PID's, UFD's and Euclidean Rings

1.27 Proposition

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

a. $\exists\, k \geq 0,\; q, r \in R[x]$ *such that*

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

PID's, UFD's and Euclidean Rings

1.27 Proposition

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

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

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

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

PID’s, UFD’s and Euclidean Rings

1.28 Theorem

$$R \quad \textit{Euclidean} \quad \Longrightarrow \quad R \quad \textit{PID.}$$

PID's, UFD's and Euclidean Rings

1.28 Theorem

$$R \quad \textit{Euclidean} \quad \Longrightarrow \quad R \quad \textit{PID}.$$

Proof:

Imitate the proof for $\mathbb{Z}$ replacing "minimal" by "minimal w.r.t. ν". $\square$

PID's, UFD's and Euclidean Rings

1.28 Theorem

$$R \quad \textit{Euclidean} \quad \Longrightarrow \quad R \quad \textit{PID}.$$

Proof:

Imitate the proof for $\mathbb{Z}$ replacing "minimal" by "minimal w.r.t. ν". □

1.29 Corollary $\mathbb{Z}$, $\mathbb{Z}[i]$, $K[x]$, $K[[x]]$, $\mathbb{R}\{x\}$ *and* $\mathbb{C}\{x\}$ *are PID's.*

PID's, UFD's and Euclidean Rings

1.28 Theorem

$$R \quad \textit{Euclidean} \quad \Longrightarrow \quad R \quad \textit{PID}.$$

Proof:

Imitate the proof for $\mathbb{Z}$ replacing "minimal" by "minimal w.r.t. ν". $\square$

1.29 Corollary $\mathbb{Z}$, $\mathbb{Z}[i]$, $K[x]$, $K[[x]]$, $\mathbb{R}\{x\}$ *and* $\mathbb{C}\{x\}$ *are PID's.*

1.30 Proposition *Let* R *be a PID,* $r \in R$.

PID's, UFD's and Euclidean Rings

1.28 Theorem

$$R \quad \textit{Euclidean} \quad \Longrightarrow \quad R \quad \textit{PID}.$$

Proof:

Imitate the proof for $\mathbb{Z}$ replacing "minimal" by "minimal w.r.t. ν". $\square$

1.29 Corollary $\mathbb{Z}$, $\mathbb{Z}[i]$, $K[x]$, $K[[x]]$, $\mathbb{R}\{x\}$ *and* $\mathbb{C}\{x\}$ *are PID's.*

1.30 Proposition *Let R be a PID, $r \in R$.*

a. r *irreducible* $\Longleftrightarrow$ $\langle r \rangle \lhd \cdot R$.

PID’s, UFD’s and Euclidean Rings

1.28 Theorem

$$R \quad \textit{Euclidean} \quad \Longrightarrow \quad R \quad \textit{PID}.$$

Proof:

Imitate the proof for $\mathbb{Z}$ replacing “minimal” by “minimal w.r.t. ν”. $\square$

1.29 Corollary $\mathbb{Z}$, $\mathbb{Z}[i]$, $K[x]$, $K[[x]]$, $\mathbb{R}\{x\}$ *and* $\mathbb{C}\{x\}$ *are PID’s.*

1.30 Proposition *Let R be a PID, $r \in R$.*

a. r *irreducible* $\Longleftrightarrow$ $\langle r \rangle \lhd \cdot R$.

b. r *irreducible* $\Longrightarrow$ r *prime.*

PID's, UFD's and Euclidean Rings

1.28 Theorem

$$R \quad \textit{Euclidean} \quad \Longrightarrow \quad R \quad \textit{PID}.$$

Proof:

Imitate the proof for $\mathbb{Z}$ replacing "minimal" by "minimal w.r.t. ν". □

1.29 Corollary $\mathbb{Z}$, $\mathbb{Z}[i]$, $K[x]$, $K[[x]]$, $\mathbb{R}\{x\}$ *and* $\mathbb{C}\{x\}$ *are PID's.*

1.30 Proposition *Let* R *be a PID,* $r \in R$.

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

b. r *irreducible* $\quad \Longrightarrow \quad r$ *prime*.

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

PID's, UFD's and Euclidean Rings

1.31 Example

$3 \in \mathbb{Z}[\sqrt{-5}] = \{x + y \cdot \sqrt{-5} \mid x, y \in \mathbb{Z}\}$ is irred., but not prime.

PID's, UFD's and Euclidean Rings

1.31 Example

$3 \in \mathbb{Z}\left[\sqrt{-5}\right] = \left\{x + y \cdot \sqrt{-5} \mid x, y \in \mathbb{Z}\right\}$ is irred., but not prime.

In particular, $\mathbb{Z}\left[\sqrt{-5}\right]$ is no PID.

PID's, UFD's and Euclidean Rings

1.31 Example

$3 \in \mathbb{Z}\left[\sqrt{-5}\right] = \left\{x + y \cdot \sqrt{-5} \;\middle|\; x, y \in \mathbb{Z}\right\}$ is irred., but not prime.

In particular, $\mathbb{Z}\left[\sqrt{-5}\right]$ is no PID.

1.32 Corollary

$$R \quad \textit{PID} \quad \Longrightarrow \quad R \quad \textit{UFD}.$$

PID's, UFD's and Euclidean Rings

1.31 Example

$3 \in \mathbb{Z}\left[\sqrt{-5}\right] = \left\{x + y \cdot \sqrt{-5} \;\middle|\; x, y \in \mathbb{Z}\right\}$ is irred., but not prime.

In particular, $\mathbb{Z}\left[\sqrt{-5}\right]$ is no PID.

1.32 Corollary

$$R \quad \textit{PID} \quad \Longrightarrow \quad R \quad \textit{UFD}.$$

1.33 Corollary $\mathbb{Z}$, $\mathbb{Z}[i]$, $K[x]$, $K[[x]]$, $\mathbb{R}\{x\}$ *and* $\mathbb{C}\{x\}$ *are UFD's.*

PID's, UFD's and Euclidean Rings

1.34 Proposition *The following are equivalent:*

PID’s, UFD’s and Euclidean Rings

1.34 Proposition *The following are equivalent:*

a. R is a UFD.

PID's, UFD's and Euclidean Rings

1.34 Proposition *The following are equivalent:*

a. R is a UFD.

b. (r irreducible $\implies$ r prime)

PID's, UFD's and Euclidean Rings

1.34 Proposition *The following are equivalent:*

a. R is a UFD.

b. (r irreducible $\implies$ r prime) and

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

PID's, UFD's and Euclidean Rings

1.34 Proposition *The following are equivalent:*

a. R is a UFD.

b. (r irreducible $\Longrightarrow$ r prime) and

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

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

PID's, UFD's and Euclidean Rings

1.34 Proposition *The following are equivalent:*

a. R is a UFD.

b. (r irreducible $\Longrightarrow$ r prime) and

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

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

PID's, UFD's and Euclidean Rings

1.34 Proposition *The following are equivalent:*

a. R is a UFD.

b. (r irreducible $\implies$ r prime) and

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

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

i.e. if $r = p_1 \cdots p_k = q_1 \cdots q_l$ with p_i, q_i irred., then

- $k = l$, and
- after reordering $\langle p_i \rangle = \langle q_i \rangle$ for all i.

1.35 Definition Let R be a UFD and $r_1, \ldots, r_k \in R$.

PID's, UFD's and Euclidean Rings

1.35 Definition Let R be a UFD and $r_1, \ldots, r_k \in R$.

a. g is a gcd (greates common divisor) of $r_1, \ldots, r_k$

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

PID's, UFD's and Euclidean Rings

1.35 Definition Let R be a UFD and $r_1, \ldots, r_k \in R$.

a. g is a gcd (greates common divisor) of $r_1, \ldots, r_k$

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

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

PID's, UFD's and Euclidean Rings

1.35 Definition Let R be a UFD and $r_1, \ldots, r_k \in R$.

a. g is a gcd (greates common divisor) of $r_1, \ldots, r_k$

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

Not.: $\gcd(r_1, \ldots, r_k) = \{g \in R \mid g \text{ is gcd of } r_1, \ldots, r_k\}$.

PID's, UFD's and Euclidean Rings

1.35 Definition Let R be a UFD and $r_1, \ldots, r_k \in R$.

a. g is a gcd (greates common divisor) of $r_1, \ldots, r_k$

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

Not.: $\mathrm{gcd}(r_1, \ldots, r_k) = \{g \in R \mid g$ is gcd of $r_1, \ldots, r_k\}$.

b. l is an lcm (lowest common multiple) of $r_1, \ldots, r_k$

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

PID's, UFD's and Euclidean Rings

1.35 Definition Let R be a UFD and $r_1, \ldots, r_k \in R$.

a. g is a gcd (greates common divisor) of $r_1, \ldots, r_k$

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

Not.: $\mathrm{gcd}(r_1, \ldots, r_k) = \{g \in R \mid g$ is gcd of $r_1, \ldots, r_k\}$.

b. l is an lcm (lowest common multiple) of $r_1, \ldots, r_k$

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

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

PID's, UFD's and Euclidean Rings

1.35 Definition Let R be a UFD and $r_1, \ldots, r_k \in R$.

a. g is a gcd (greates common divisor) of $r_1, \ldots, r_k$

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

Not.: $\mathrm{gcd}(r_1, \ldots, r_k) = \{g \in R \mid g$ is gcd of $r_1, \ldots, r_k\}$.

b. l is an lcm (lowest common multiple) of $r_1, \ldots, r_k$

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

Not.: $\mathrm{lcm}(r_1, \ldots, r_k) = \{l \in R \mid l$ is lcm of $r_1, \ldots, r_k\}$.

PID's, UFD's and Euclidean Rings

1.36 Remark Let R be a PID.

PID's, UFD's and Euclidean Rings

1.36 Remark Let R be a PID.

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

PID’s, UFD’s and Euclidean Rings

1.36 Remark Let R be a PID.

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

and

$$l \in \mathrm{lcm}(r_1, \dots, r_k) \quad \Longleftrightarrow \quad \langle l \rangle = \langle r_1 \rangle \cap \dots \cap \langle r_k \rangle.$$

PID's, UFD's and Euclidean Rings

1.36 Remark Let R be a PID.

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

and

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

1.37 Lemma *Let R be an ID and $r \in R$.*

PID's, UFD's and Euclidean Rings

1.36 Remark Let R be a PID.

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

and

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

1.37 Lemma *Let R be an ID and $r \in R$.*

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

PID's, UFD's and Euclidean Rings

1.36 Remark Let R be a PID.

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

and

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

1.37 Lemma *Let R be an ID and $r \in R$.*

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

b. r *irreducible in* $R \implies r$ *irreducible in* $R[x]$.

PID's, UFD's and Euclidean Rings

1.36 Remark Let R be a PID.

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

and

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

1.37 Lemma *Let R be an ID and $r \in R$.*

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

b. *r irreducible in R $\Longrightarrow$ r irreducible in $R[x]$.*

c. *r prime in R $\Longrightarrow$ r prime in $R[x]$.*

PID's, UFD's and Euclidean Rings

1.38 Theorem (Lemma of Gauß)

$$R \text{ a } UFD \quad \Longrightarrow \quad R[x] \text{ a } UFD.$$

PID's, UFD's and Euclidean Rings

1.38 Theorem (Lemma of Gauß)

$$R \text{ a UFD} \implies R[x] \text{ a UFD.}$$

1.39 Corollary K a *field* $\implies K[x_1, \ldots, x_n]$ a *UFD*.

PID's, UFD's and Euclidean Rings

1.38 Theorem (Lemma of Gauß)

$$R \text{ a } \textit{UFD} \quad \Longrightarrow \quad R[x] \text{ a } \textit{UFD}.$$

1.39 Corollary K a *field* $\Longrightarrow$ $K[x_1, \ldots, x_n]$ a *UFD*.

1.40 Corollary $R[x]$ *is a PID* $\Longleftrightarrow$ R *is a field*.

PID's, UFD's and Euclidean Rings

1.38 Theorem (Lemma of Gauß)

$$R \text{ a UFD} \implies R[x] \text{ a UFD.}$$

1.39 Corollary K a *field* $\implies$ $K[x_1, \ldots, x_n]$ a *UFD*.

1.40 Corollary $R[x]$ *is a PID* $\iff$ R *is a field.*

In particular, $K[x_1, \ldots, x_n]$ *is not a PID for* $n \geq 2$.

PID's, UFD's and Euclidean Rings

1.38 Theorem (Lemma of Gauß)

$$R \text{ a } \textit{UFD} \quad \Longrightarrow \quad R[x] \text{ a } \textit{UFD}.$$

1.39 Corollary K a *field* $\quad \Longrightarrow \quad K[x_1, \ldots, x_n]$ a *UFD*.

1.40 Corollary $R[x]$ *is a PID* $\quad \Longleftrightarrow \quad R$ *is a field.*

In particular, $K[x_1, \ldots, x_n]$ *is not a PID for* $n \geq 2$.

1.41 Theorem

$$\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right] \text{ is a PID, but not Euclidean.}$$

PID's, UFD's and Euclidean Rings

1.45 Remark

We have seen in Theorem 1.41, Corollary 1.39 and 1.40 that:

$$R \text{ is Euclidean} \implies R \text{ is a PID} \implies R \text{ is a UFD},$$

but

$$R \text{ is Euclidean} \not\Longleftarrow R \text{ is a PID} \not\Longleftarrow R \text{ is a UFD}.$$

PID's, UFD's and Euclidean Rings

1.42 Proposition *Let R be an ID.*

Then R is a PID $\iff$ $\exists\ \alpha : R \to \mathbb{N}$ such that

PID's, UFD's and Euclidean Rings

1.42 Proposition *Let R be an ID.*

Then R is a PID $\iff$ $\exists\, \alpha : R \to \mathbb{N}$ *such that*

$$\forall\, 0 \neq b \not|\, a \quad \exists\, u, v \in R \;:\; \alpha(0) < \alpha(ua - vb) < \alpha(b).$$

PID’s, UFD’s and Euclidean Rings

1.42 Proposition *Let R be an ID.*

Then R is a PID $\iff$ $\exists\, \alpha : R \to \mathbb{N}$ *such that*

$$\forall\, 0 \neq b \not| \, a \quad \exists\, u, v \in R \; : \; \alpha(0) < \alpha(ua - vb) < \alpha(b).$$

Idea: $g = ua - vb \in \gcd(a, b)$ and $\langle g \rangle = \langle a, b \rangle$!

PID's, UFD's and Euclidean Rings

1.42 Proposition *Let R be an ID.*

Then R is a PID $\iff$ $\exists\, \alpha : R \to \mathbb{N}$ *such that*

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

Idea: $g = ua - vb \in \mathrm{gcd}(a, b)$ and $\langle g \rangle = \langle a, b \rangle$!

1.43 Proposition R *be* ***Euclidean****,* $0 \neq p \in R \setminus R^*$ ***minimal*** *w.r.t* ν*,* $\pi : R \to R/\langle p \rangle : a \mapsto \overline{a}$*. Then:*

PID's, UFD's and Euclidean Rings

1.42 Proposition *Let R be an ID.*

Then R is a PID $\iff$ $\exists\, \alpha : R \to \mathbb{N}$ *such that*

$$\forall\, 0 \neq b \not| \, a \quad \exists\, u, v \in R \ : \ \alpha(0) < \alpha(ua - vb) < \alpha(b).$$

Idea: $g = ua - vb \in \mathrm{gcd}(a, b)$ and $\langle g \rangle = \langle a, b \rangle$!

1.43 Proposition R *be* ***Euclidean***, $0 \neq p \in R \setminus R^*$ ***minimal*** *w.r.t* ν, $\pi : R \to R/\langle p \rangle : a \mapsto \overline{a}$. *Then:*

a. p *is* ***prime*** & $K = R/\langle p \rangle$ *is a* ***field***.

PID's, UFD's and Euclidean Rings

1.42 Proposition *Let R be an ID.*

Then R is a PID $\iff$ $\exists\, \alpha : R \to \mathbb{N}$ *such that*

$$\forall\, 0 \neq b \not| a \quad \exists\, u, v \in R \;:\; \alpha(0) < \alpha(ua - vb) < \alpha(b).$$

Idea: $g = ua - vb \in \gcd(a, b)$ and $\langle g \rangle = \langle a, b \rangle$!

1.43 Proposition R *be Euclidean*, $0 \neq p \in R \setminus R^*$ *minimal w.r.t* ν, $\pi : R \to R/\langle p \rangle : a \mapsto \overline{a}$. *Then:*

a. p *is prime* & $K = R/\langle p \rangle$ *is a field.*

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

PID's, UFD's and Euclidean Rings

1.42 Proposition *Let R be an ID.*

Then R is a PID $\iff$ $\exists\, \alpha : R \to \mathbb{N}$ *such that*

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

Idea: $g = ua - vb \in \gcd(a, b)$ and $\langle g \rangle = \langle a, b \rangle$!

1.43 Proposition R be *Euclidean*, $0 \neq p \in R \setminus R^*$ *minimal* w.r.t ν, $\pi : R \to R/\langle p \rangle : a \mapsto \overline{a}$. *Then:*

a. p is *prime* & $K = R/\langle p \rangle$ is a *field*.

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

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

PID's, UFD's and Euclidean Rings

Proof of Theorem 1.41, see [Bru00]:

Define a *Norm* $N : R \to \mathbb{N}$ on $R = \mathbb{Z}[\omega]$, $\omega = \frac{1+\sqrt{-19}}{2}$ by

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

PID's, UFD's and Euclidean Rings

Proof of Theorem 1.41, see [Bru00]:

Define a *Norm* $N : R \to \mathbb{N}$ on $R = \mathbb{Z}[\omega]$, $\omega = \frac{1+\sqrt{-19}}{2}$ by

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

PID's, UFD's and Euclidean Rings

Proof of Theorem 1.41, see [Bru00]:

Define a *Norm* $N : R \to \mathbb{N}$ on $R = \mathbb{Z}[\omega]$, $\omega = \frac{1+\sqrt{-19}}{2}$ by

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

PID's, UFD's and Euclidean Rings

Proof of Theorem 1.41, see [Bru00]:

Define a *Norm* $N : R \to \mathbb{N}$ on $R = \mathbb{Z}[\omega]$, $\omega = \frac{1+\sqrt{-19}}{2}$ by

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

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

PID's, UFD's and Euclidean Rings

Proof of Theorem 1.41, see [Bru00]:

Define a *Norm* $N : R \to \mathbb{N}$ on $R = \mathbb{Z}[\omega]$, $\omega = \frac{1+\sqrt{-19}}{2}$ by

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

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

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

PID's, UFD's and Euclidean Rings

Proof of Theorem 1.41, see [Bru00]:

Define a *Norm* $N : R \to \mathbb{N}$ on $R = \mathbb{Z}[\omega]$, $\omega = \frac{1+\sqrt{-19}}{2}$ by

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

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

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

Thus:

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

Proof of Theorem 1.41, see [Bru00]:

Define a *Norm* $N : R \to \mathbb{N}$ on $R = \mathbb{Z}[\omega]$, $\omega = \frac{1+\sqrt{-19}}{2}$ by

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

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

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

And hence if $x = a + b \cdot \omega$:

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

PID’s, UFD’s and Euclidean Rings

Claim: 2 and 3 are irreducible.

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

PID’s, UFD’s and Euclidean Rings

Claim: 2 and 3 are irreducible.

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

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

PID's, UFD's and Euclidean Rings

Claim: 2 and 3 are irreducible.

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

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

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

PID's, UFD's and Euclidean Rings

Claim: 2 and 3 are irreducible.

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

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

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

PID's, UFD's and Euclidean Rings

Claim: 2 and 3 are irreducible.

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

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

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

$$\Longrightarrow \quad b = 0$$

PID's, UFD's and Euclidean Rings

Claim: 2 and 3 are irreducible.

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

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

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

$$\Longrightarrow \quad b = 0 \quad \Longrightarrow \quad a^2 = 2 \;\; \& \;\; a \in \mathbb{Z} \quad ⚡⚡⚡$$

PID's, UFD's and Euclidean Rings

Claim: 2 and 3 are irreducible.

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

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

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

$$\Longrightarrow \quad b = 0 \quad \Longrightarrow \quad a^2 = 2 \;\; \& \;\; a \in \mathbb{Z} \quad ↯↯↯$$

The proof for 3 works analogously.

PID's, UFD's and Euclidean Rings

Claim: R is not Euclidean.

PID’s, UFD’s and Euclidean Rings

Claim: R is not Euclidean.

Suppose R was Euclidean and choose $p \in R$ as in 1.43.

PID's, UFD's and Euclidean Rings

Claim: R is not Euclidean.

Suppose R was Euclidean and choose $p \in R$ as in 1.43.

I.e. $0 \neq p \in R$ minimal w.r.t. ν and then

- p is prime.
- $K = R/\langle p \rangle$ is field.
- $a \in R \quad \Longrightarrow \quad a = q \cdot p + r$ with $r = 0$ or $r \in R^*$.
- $|K^*| \leq |R^*|$.

PID's, UFD's and Euclidean Rings

Claim: R is not Euclidean.

Suppose R was Euclidean and choose $p \in R$ as in 1.43.

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

PID's, UFD's and Euclidean Rings

Claim: R is not Euclidean.

Suppose R was Euclidean and choose $p \in R$ as in 1.43.

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

Note:

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

and

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

PID’s, UFD’s and Euclidean Rings

Claim: R is not Euclidean.

Suppose R was Euclidean and choose $p \in R$ as in 1.43.

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

Hence:

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

PID's, UFD's and Euclidean Rings

Claim: R is not Euclidean.

Suppose R was Euclidean and choose $p \in R$ as in 1.43.

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

Hence:

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

In particular:

$$2 = q \cdot p + r \quad \text{with } r \neq 0$$

PID's, UFD's and Euclidean Rings

Claim: R is not Euclidean.

Suppose R was Euclidean and choose $p \in R$ as in 1.43.

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

Hence:

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

In particular:

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

PID's, UFD's and Euclidean Rings

Claim: R is not Euclidean.

Suppose R was Euclidean and choose $p \in R$ as in 1.43.

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

Hence:

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

In particular:

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

$$\Longrightarrow \quad \left\{ \begin{array}{ll} q \cdot p = 1 & ↯↯↯ \text{ to } p \text{ prime,} \\ & \end{array} \right.$$

PID’s, UFD’s and Euclidean Rings

Claim: R is not Euclidean.

Suppose R was Euclidean and choose $p \in R$ as in 1.43.

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

Hence:

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

In particular:

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

$$\Longrightarrow \quad \begin{cases} q \cdot p = 1 & ⚡⚡⚡ \text{ to } p \text{ prime,} \\ q \cdot p = 3 \;\Rightarrow\; p \mid 3 & ⚡⚡⚡ \text{ to } 3 \text{ irred. \& } \langle p\rangle \neq \langle 3\rangle. \end{cases}$$

PID’s, UFD’s and Euclidean Rings

Claim:

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

PID's, UFD's and Euclidean Rings

Claim:

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

Note:

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

$$1 \in \gcd(a, q) \text{ and } 1 \in \gcd(b, s)$$

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

PID's, UFD's and Euclidean Rings

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

PID's, UFD's and Euclidean Rings

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

If $u', v' \in R$ such that

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

PID's, UFD's and Euclidean Rings

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

If $u', v' \in R$ such that

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

then $u = u'$ and $v = v' + u' \cdot (a' + b' \cdot \omega)$ works, since

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

PID's, UFD's and Euclidean Rings

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

If $u', v' \in R$ such that

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

then $u = u'$ and $v = v' + u' \cdot (a' + b' \cdot \omega)$ works, since

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

PID's, UFD's and Euclidean Rings

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

If $u', v' \in R$ such that

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

then $u = u'$ and $v = v' + u' \cdot (a' + b' \cdot \omega)$ works, since

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

We may, therefore, assume that $a' = b' = 0$.

PID's, UFD's and Euclidean Rings

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

- $0 \leq a < q$,
- $0 \leq b < s$,
- $1 \in \gcd(a, q)$, and
- $1 \in \gcd(b, s)$.

PID's, UFD's and Euclidean Rings

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

1^{st} **Case** $b = 0$: Then $u = 1$ and $v = 0$ works.

PID's, UFD's and Euclidean Rings

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

1^{st} **Case** $b = 0$: Then $u = 1$ and $v = 0$ works.

2^{nd} **Case** $b \neq 0$, $q \not| s$: Then

$$q \not| s \cdot a \Longrightarrow \exists\, 0 < d < q,\ c \in \mathbb{Z} \ :\ sa = cq + d,$$

PID's, UFD's and Euclidean Rings

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

1^{st} **Case** $b = 0$: Then $u = 1$ and $v = 0$ works.

2^{nd} **Case** $b \neq 0$, $q \not| s$: Then

$$q \not| s \cdot a \Longrightarrow \quad \exists\, 0<d<q,\ c \in \mathbb{Z} \ :\ sa = cq + d,$$

and $u = s$ and $v = c + b\omega$ works:

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

PID's, UFD's and Euclidean Rings

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

1^{st} **Case** $b = 0$: Then $u = 1$ and $v = 0$ works.

2^{nd} **Case** $b \neq 0$, $q \nmid s$: Then $u = s$ and $v = c + b\omega$ works.

3^{rd} **Case** $b \neq 0$, $q \mid s$, $s > 2$:

PID's, UFD's and Euclidean Rings

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

3^{rd} **Case** $b \neq 0$, $q \mid s$, $s > 2$: Then

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

PID’s, UFD’s and Euclidean Rings

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

3^{rd} **Case** $b \neq 0$, $q \mid s$, $s > 2$: Then

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

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

for suitable $l, k, a_1, a_2 \in \mathbb{Z}$ such that $\left| \frac{a_1}{a_2} \right| \leq \frac{1}{2}$.

PID's, UFD's and Euclidean Rings

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

3^{rd} **Case** $b \neq 0$, $q \mid s$, $s > 2$:

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

Then $u = m$ and $v = l + k\omega$ works:

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

PID's, UFD's and Euclidean Rings

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

3^{rd} **Case** $b \neq 0$, $q \mid s$, $s > 2$:

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

Then $u = m$ and $v = l + k\omega$ works:

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

PID's, UFD's and Euclidean Rings

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

3^{rd} **Case** $b \neq 0$, $q \mid s$, $s > 2$:

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

Then $u = m$ and $v = l + k\omega$ works:

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

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

PID's, UFD's and Euclidean Rings

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

3^{rd} **Case** $b \neq 0$, $q \mid s$, $s > 2$:

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

Then $u = m$ and $v = l + k\omega$ works:

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

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

PID's, UFD's and Euclidean Rings

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

1^{st} **Case** $b = 0$: Then $u = 1$ and $v = 0$ works.

2^{nd} **Case** $b \neq 0$, $q \not| s$: Then $u = s$ and $v = c + b\omega$ works.

3^{rd} **Case** $b \neq 0$, $q \mid s$, $s > 2$: Then $u = m$, $v = l + k\omega$ works.

4^{th} **Case** $b \neq 0$, $q \mid s$, $s = 2$:

PID's, UFD's and Euclidean Rings

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

4^{th} **Case** $b \neq 0$, $q \mid s$, $s = 2$: Then $q = s = 2$

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

PID's, UFD's and Euclidean Rings

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

4^{th} **Case** $b \neq 0$, $q \mid s$, $s = 2$: Then $q = s = 2$

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

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

PID's, UFD's and Euclidean Rings

This proves the claim:

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

PID's, UFD's and Euclidean Rings

This proves the claim:

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

and hence

Proposition 1.42 with $\alpha = N \implies R$ is a PID!

□

PID's, UFD's and Euclidean Rings

1.45 Remark

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

PID's, UFD's and Euclidean Rings

1.45 Remark

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

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

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

PID's, UFD's and Euclidean Rings

1.45 Remark

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

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

c. $\mathbb{Z}[\omega_d]$ is a UFD $\iff$ $\mathbb{Z}[\omega_d]$ is a PID.

PID's, UFD's and Euclidean Rings

1.45 Remark

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

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

c. $\mathbb{Z}[\omega_d]$ is a UFD $\iff$ $\mathbb{Z}[\omega_d]$ is a PID.

d. If $d \leq -1$ then

PID's, UFD's and Euclidean Rings

1.45 Remark

a. $|K : \mathbb{Q}| = 2 \quad \Longleftrightarrow \quad K = \mathbb{Q}\big[\sqrt{d}\big], 0, 1 \neq d \in \mathbb{Z}$ squarefree.

b. $\mathbb{Z}[\omega_d] = \big\{a \in \mathbb{Q}\big[\sqrt{d}\big] \;\big|\; a \text{ integral}\big\}$

c. $\mathbb{Z}[\omega_d]$ is a UFD $\quad \Longleftrightarrow \quad$ $\mathbb{Z}[\omega_d]$ is a PID.

d. If $d \leq -1$ then

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

PID's, UFD's and Euclidean Rings

1.45 Remark

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

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

c. $\mathbb{Z}[\omega_d]$ is a UFD $\iff$ $\mathbb{Z}[\omega_d]$ is a PID.

d. If $d \leq -1$ then

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

and

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

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.