LECTURE NOTES IN COMMUTATIVE ALGEBRA

THOMAS MARKWIG

1 Rings and Modules

C) **Euclidean Rings, PID's and UFD's**

1.23 Definition

Let R be an integral domain, $r, r' \in R$.

a. r *divides* r' if and only if

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

if and only if

$$\langle r' \rangle \subseteq \langle r \rangle.$$

We denote this by $r \mid r'$.

b. r is *irreducible* if and only if

$$0 \neq r \notin R^* \quad \text{and} \quad (r = s \cdot t \;\Rightarrow\; s \in R^* \;\text{ or }\; t \in R^*).$$

c. r is *prime* if and only if

$$0 \neq r \notin R^* \quad \text{and} \quad (r \mid s \cdot t \;\Rightarrow\; r \mid s \;\text{ or }\; r \mid t)$$

if and only if

$$\langle 0 \rangle \neq \langle r \rangle \text{ is a prime ideal.}$$

d. r and r' are *associated* if and only if

$$\exists\, u \in R^* \;:\; r = r' \cdot u$$

if and only if

$$\langle r \rangle = \langle r' \rangle.$$

1.24 Example a. If r is prime, then r is irreducible.

Proof: If $r = s \cdot t$, then $r \mid s \cdot t$, and since r is prime we thus may assume $r \mid s$. Hence there is a $u \in R$ such that $s = u \cdot r$, and therefore $r = r \cdot u \cdot t$. Cancelling out the non-zerodivisor r we get $1 = u \cdot t$, that is, $t \in R^*$. $\square$

b. If r and s are irreducible and $r \mid s$, then r and s are associated.

Proof: If $r \mid s$, then $s = r \cdot t$ for some $t \in R$. But since s is irreducible, t or r must be a unit. Since r is irreducible, it is not a unit. Thus t is a unit, and r and s are associated. $\square$

c. If $R = \mathbb{Z}$ is the ring of integers, then:

$$p \text{ is irreducible } \iff p \text{ is prime } \iff p \text{ is a prime number.}$$

d. If $R = K[x]$, where K is a field, then by Proposition 1.30:

$$p \text{ is prime } \iff p \text{ is an irreducible polynomial.}$$

e. If $R = K[[x]]$, where K is a field, then by Proposition 1.30:

$$p \text{ is prime } \Leftrightarrow p \text{ is irreducible } \Leftrightarrow p = u \cdot x \text{ for some unit } u \quad \Leftrightarrow \operatorname{ord}(p) = 1.$$

1.25 Definition
Let R be an integral domain.

a. R is a *Euclidean ring* if and only if there is a function $\nu : R \setminus \{0\} \to \mathbb{N}$ such that

$$\forall\, a, b \in R \setminus \{0\} \;\; \exists\, q, r \in R \;:\; a = q \cdot b + r \text{ with } r = 0 \text{ or } 0 \le \nu(r) < \nu(b).$$

We call this decomposition of a a *division with remainder* (short: DwR) of a with respect to b.

b. R is a *principle ideal domain* (short: PID) if and only if every ideal in R is principle.

c. R is a *unique factorisation domain* (short: UFD) or *factorial* if and only if every $0 \neq r \in R \setminus R^*$ is a product of finitely many prime elements.

1.26 Example a. $R = \mathbb{Z}$ is a Euclidean ring with $\nu(z) = |z|$ due to the usual DwR in $\mathbb{Z}$.

b. $R = K[x]$, where K is a field, is a Euclidean ring with $\nu(f) = \deg(f)$ by Proposition 1.27.

c. $R \in \{K[[x]], \mathbb{R}\{x\}, \mathbb{C}\{x\} \mid K \text{ is a field}\}$, is a Euclidean ring with $\nu(f) = \operatorname{ord}(f)$.

Proof: Given $a, b \in R$ we can write them uniquely as $a = u \cdot x^n$ respectively $b = v \cdot x^m$ for some units $u, v \in K[[x]]^*$ and where $n = \operatorname{ord}(a)$ and $m = \operatorname{ord}(b)$. If $n < m$, then $a = 0 \cdot b + a$ is the desired decomposition, while if $n \ge m$, then $a = (u \cdot x^{n-m} \cdot v^{-1}) \cdot b + 0$ is. $\square$

d. $R = \mathbb{Z}[i] = \{x + i \cdot y \mid x, y \in \mathbb{Z}\} \le \mathbb{C}$ is a Euclidean ring with $\nu(x + i \cdot y) = |x + iy|^2 = x^2 + y^2$.

Proof: Let $a, b \in \mathbb{Z}[i]$, $b \neq 0$, be given. Then the complex number $\frac{a}{b} = u + i \cdot v$ for some real numbers $u, v \in \mathbb{R}$. Approximating u and v by integers we find $m, n \in \mathbb{Z}$ such that $|u - m| \leq \frac{1}{2}$ and $|v - n| \leq \frac{1}{2}$. Setting $q := m + i \cdot n \in \mathbb{Z}[i]$ and $r := a - q \cdot b \in \mathbb{Z}[i]$ we have

$$\nu(r) = |a - qb|^2 = |b|^2 \cdot \big((u-m)^2 + (v-n)^2\big) \leq \frac{1}{2} \cdot |b|^2 < \nu(b)$$

and $a = q \cdot b + r$. □

1.27 Proposition (Division with Remainder)
Let R be a ring, $f = \sum_{i=0}^n f_i x^i, g = \sum_{i=0}^m g_i x^i \in R[x]$ such that $f_n \neq 0 \neq g_m$.

a. *Then* $\exists\, k \geq 0,\ q, r \in R[x]$ *such that* $f_n^k \cdot g = q \cdot f + r$ *and* $\deg(r) < \deg(f)$.

b. *If R is an ID and $f_n \in R^*$, then there are unique $q, r \in R[x]$ such that $g = q \cdot f + r$ and* $\deg(r) < \deg(f)$.

Proof: a. We do the proof by induction on $m = \deg(g)$.
Note, if $m = n = 0$, then we are done with $k = 1$, $q = g$ and $r = 0$, and if $0 \leq m < n$, we may set $k = 0$, $q = 0$ and $r = g$.
We thus may assume that $m > 0$ and $n \leq m$. Set

$$g' := f_n \cdot g - g_m \cdot x^{m-n} \cdot f.$$

Then $\deg(g') < \deg(g) = m$ and by induction there are $q', r' \in R[x]$ and $k' \geq 0$ such that

$$q' \cdot f + r' = f_n^{k'} \cdot g' = f_n^{k'+1} \cdot g - f_n^{k'} \cdot g_m \cdot x^{m-n} \cdot f$$

and $\deg(r') < \deg(f)$. This implies

$$f_n^{k'+1} \cdot g = \big(q' + f_n^{k'} \cdot g_m \cdot x^{m-n}\big) \cdot f + r',$$

and we are done setting $k = k' + 1$, $q = q' + f_n^{k'} \cdot g_m \cdot x^{m-n}$, and $r = r'$.

b. The existence of the decomposition follows from a., since f_n is invertible. As for the uniqueness suppose that

$$g = q \cdot f + r = q' \cdot f + r'$$

with $q, q', r, r' \in R[x]$ and $\deg(r), \deg(r') < \deg(f)$. Then

$$\deg(q - q') \cdot \deg(f) = \deg(r' - r) \leq \max\{\deg(r), \deg(r')\} < \deg(f),$$

which implies that $q - q' = 0$. But then $q = q'$ and hence $r = r'$.

□

1.28 Theorem
If R is a Euclidean ring, then R is a PID.

Proof: Let $0 \neq I \trianglelefteq R$ be an ideal. Then there is a $0 \neq a \in I$ such that $\nu(a)$ is minimal. We claim that $I = \langle a \rangle$, where "$\supseteq$" is clear.
Let $b \in I$, then there are $q, r \in R$ such that $b = q \cdot a + r$ and $r = 0$ or $\nu(r) < \nu(a)$. Since $r = b - q \cdot a \in I$ and $\nu(a)$ was minimal, we conclude that $r = 0$. Thus $b = q \cdot a \in \langle a \rangle$. $\square$

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 and $0 \neq r \in R$.

a. *r is irreducible if and only if $\langle r \rangle \lhd \cdot R$.*
b. *If r is irreducible, then r is prime.*
c. $\operatorname{Spec}(R) = \mathfrak{m} - \operatorname{Spec}(R) \cup \{\langle 0 \rangle\}$.

Proof: a. Assume first that r is irreducible. If $\langle r \rangle \subseteq \langle s \rangle \subseteq R$, then there is a $t \in R$ such that $r = s \cdot t$. Since r is irreducible either s is a unit or t is. But thus $\langle s \rangle = R$ or $\langle s \rangle = \langle r \rangle$, and hence $\langle r \rangle$ is maximal.
Assume now that $\langle r \rangle$ is maximal. If $r = s \cdot t$, then $\langle r \rangle \subseteq \langle s \rangle \subseteq R$ and by assumption either $\langle r \rangle = \langle s \rangle$ or $\langle s \rangle = R$. In the first case t must be a unit, in the latter case s must be. In any case, this implies that r is irreducible.

b. If r is irreducible, then by a. $\langle r \rangle$ is a maximal ideal. Thus it is a prime ideal, and therefore r is a prime element.

c. It suffices to show that every non-zero prime ideal is maximal. But if $0 \neq P \in \operatorname{Spec}(R)$, then $P = \langle r \rangle$, since R is a PID. Thus r must be prime and we have already seen that every prime element is irreducible. By a. therefore $P \in \mathfrak{m} - \operatorname{Spec}(R)$.

$\square$

1.31 Example
Let $R = \mathbb{Z}\big[\sqrt{-5}\big] = \big\{x + y \cdot \sqrt{-5} \;\big|\; x, y \in \mathbb{Z}\big\}$. We claim that $3 \in R$ is irreducible, but not prime. In particular, R is no PID and the converse of Proposition 1.30 b. is in general wrong.
Show first that $R^* = \{1, -1\} = \{r \in R \mid |r|^2 = 1\}$. For this let $r = x + y \cdot \sqrt{-5} \in R^*$ be given, and let $s \in R$ be its inverse. Then

$$1 = |r \cdot s|^2 = |r|^2 \cdot |s|^2 = (x^2 + 5 \cdot y^2) \cdot |s|^2,$$

and since $|s|^2 \geq 1$ it follows that $x^2 = 1$ and $y^2 = 0$. Hence $r \in \{1, -1\}$.

We next show that 3 is irreducible. Suppose that $3 = r \cdot s$ with $r = x + y \cdot \sqrt{-5}$, $s \notin R^*$. In particular $|r|^2$ and $|s|^2$ are integers strictly greater than one and thus

$$9 = 3^2 = |r \cdot s|^2 = |r|^2 \cdot |s|^2$$

implies that $x^2 + 5y^2 = |r|^2 = |s|^2 = 3$. This is, however, a contradiction to $x, y \in \mathbb{Z}$. We finally show that 3 is not a prime. Note that

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

Suppose that $3 \mid \big(2 + \sqrt{-5}\big)$ in R, then there is an $r = x + y \cdot \sqrt{-5} \in R$ such that $3 \cdot r = 2 + \sqrt{-5}$ and hence

$$9 \cdot |r|^2 = |2 + \sqrt{-5}|^2 = 9.$$

This implies that $x^2 + 5y^2 = |r|^2 = 1$ and hence $r \in \{1, -1\}$, which clearly contradicts the fact that $3 \cdot r = 2 + \sqrt{-5}$. Thus $3 \not| \big(2 + \sqrt{-5}\big)$, and similarly $3 \not| \big(2 - \sqrt{-5}\big)$. This, however, shows that 3 is not a prime.

1.32 Corollary

If R is a PID, then R is a UFD.

Proof: Let $\mathcal{M} = \{\langle r \rangle \mid 0 \neq r \in R \setminus R^*, r \text{ is not a finite product of irreducibles}\}$. Suppose that $\mathcal{M} \neq \emptyset$. If

$$\langle r_1 \rangle \subseteq \langle r_2 \rangle \subseteq \langle r_3 \rangle \subseteq \ldots$$

is a chain in $\mathcal{M}$, then

$$I = \bigcup_{i=1}^{\infty} \langle r_i \rangle \trianglelefteq R$$

is an ideal in R. Since R is a PID we have $I = \langle s \rangle$ for some $s \in R$. But then there is some i such that $s \in \langle r_i \rangle$ and thus $I = \langle s \rangle \subseteq \langle r_i \rangle \subseteq I$. This shows $I = \langle r_i \rangle \in \mathcal{M}$ is an upper bound of this chain in $\mathcal{M}$.

By Zorn's Lemma there must be a $\langle r \rangle \in \mathcal{M}$ which is maximal in $\mathcal{M}$. Since $\langle r \rangle \in \mathcal{M}$ we know that r is not irreducible. Thus there are $s, t \in R \setminus R^*$ such that $r = s \cdot t$. This implies

$$\langle r \rangle \subsetneqq \langle s \rangle \quad \text{and} \quad \langle r \rangle \subsetneqq \langle t \rangle.$$

Due to the maximality of $\langle r \rangle$ we conclude that $\langle s \rangle, \langle t \rangle \notin \mathcal{M}$. In particular, there are irreducible elements $p_1, \ldots, p_k, q_1, \ldots, q_l \in R$ such that $s = p_1 \cdots p_k$ and $t = q_1 \ldots q_l$. But then

$$r = s \cdot t = p_1 \cdots p_k \cdot q_1 \ldots q_l$$

is a product of finitely many irreducible elements in contradiction to $\langle r \rangle \in \mathcal{M}$. Hence $\mathcal{M} = \emptyset$ and each $0 \neq r \in R \setminus R^*$ is a finite product of irreducible elements. By Proposition 1.30 it thus is also a finite product of prime elements and R is factorial. $\square$

1.33 Corollary

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

1.34 Proposition

The following statements are equivalent:

a. *R is a UFD.*

b. *Every $0 \neq r \in R \setminus R^*$ is a finite product of irreducible elements and every irreducible element is prime.*

c. *Every $0 \neq r \in R \setminus R^*$ is a finite product of irreducible elements in a unique way, i.e. if $r = p_1 \cdots p_k = q_1 \cdots q_l$ with p_i and q_i irreducible for all i, then $k = l$ and there is a permutation $\sigma \in \mathrm{Sym}(k)$ such that p_i and $q_{\sigma(i)}$ are associated.*

Proof: Let us first show that a. implies b.. We have already seen that any prime element is irreducible. Thus if R is a UFD and $0 \neq r \in R \setminus R^*$, then r is a finite product of irreducible elements. It remains to show that if r is irreducible, then r is prime. However, since R is a UFD we can write $r = p_1 \cdots p_k$ for prime elements p_i, and since r is irreducible and the p_i are no units, we conclude that $k = 1$ and $r = p_1$ is prime.

We next show that b. implies c.. Let $r = p_1 \cdots p_k = q_1 \cdots q_l$ with p_i and q_i irreducible and assume that k is the minimal number such that r can be decomposed into k irreducible factors. We show by induction on k that $k = l$ and that $\sigma \in \mathrm{Sym}(k)$ exists as claimed. If $k = 1$, then $r = p_1 = q_1 \cdots q_l$ is irreducible and since the q_i are no units we conclude $l = 1$ and $r = p_1 = q_1$. If $k > 1$, then

$$p_k \mid p_1 \cdots p_k = q_1 \cdots q_l,$$

and since p_k is prime we conclude that $p_k \mid q_i$ for some i. Since p_k and q_i are both irreducible, they must be associated, i.e. $q_i = u \cdot p_k$ for some unit u. W.l.o.g. we may assume $i = l$ (this means applying a suitable σ to the indices). Thus

$$p_1 \cdots p_{k-1} = q_1 \cdots q_{l-1} \cdot u^{-1},$$

and by induction we are done by induction.

Let us finally show that c. implies a.. It suffices to show that every irreducible element is prime. Let p be irreducible and $p \mid s \cdot t$. By assumption s and t can be decomposed uniquely into products of irreducible elements, say

$$s = p_1 \cdots p_k \quad \text{and } t = p_{k+1} \cdots p_l.$$

Thus $p \mid p_1 \cdots p_l$, and uniqueness implies the p must be associated some p_i. In particular $p \mid p_i$ and thus divides s or t. $\square$

1.35 Definition

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

a. We call $g \in R$ **a** *greatest common divisor* (short: gcd) of $r_1, \ldots, r_k$ if and only if

$$g \mid r_i \quad \forall\, i = 1, \ldots, k \quad \text{and} \quad (t \mid r_i \quad \forall\, i = 1, \ldots, k \implies t \mid g)$$

if and only if

$$g \mid r_i \quad \forall\, i = 1, \ldots, k \quad \text{and} \quad \nexists\, p \text{ irreducible such that } p \mid \frac{r_i}{g} \quad \forall\, i = 1, \ldots, k.$$

Notation: $\gcd(r_1, \ldots, r_k) = \{g \in R \mid g \text{ is a greatest common divisor of } r_1, \ldots, r_k\}$. Obviously, $1 \in \gcd(r_1, \ldots, r_k)$ if and only if $\gcd(r_1, \ldots, r_k) = R^*$, and in this case we say that the r_i *have no common divisor*.

b. We call $l \in R$ **a** *lowest common multiple* (short: lcm) of $r_1, \ldots, r_k$ if and only if

$$r_i \mid l \quad \forall\, i = 1, \ldots, k \quad \text{and} \quad (r_i \mid t \quad \forall\, i = 1, \ldots, k \implies l \mid t),$$

and in case $k = 2$ this holds if and only if

$$r_1, r_2 \mid l \quad \text{and} \quad \frac{r_1 \cdot r_2}{l} \in \gcd(r_1, r_2).$$

Notation: $\operatorname{lcm}(r_1, \ldots, r_k) = \{l \in R \mid l \text{ is a lowest common multiple of } r_1, \ldots, r_k\}$.

1.36 Remark

If R is a PID, then:

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

and

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

Proof: The proof is an easy exercise using the definition and induction on k. □

1.37 Lemma

Let R be an ID.

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

b. *If $r \in R$ is irreducible in R, it is irreducible in $R[x]$.*

c. *If $r \in R$ is prime in R, it is prime in $R[x]$.*

Proof: a. Clearly, $R^* \subseteq R[x]^*$. Let therefore $f \in R[x]^*$. Then there is a $g \in R[x]$ such that $f \cdot g = 1$, and by the degree formula we have

$$0 = \deg(1) = \deg(f \cdot g) = \deg(f) + \deg(g).$$

This implies $f, g \in R$, and therefore $f \in R^*$.

b. If $r = s \cdot t$ for $s, t \in R[x]$, then by the degree formula in integral domains we have

$$0 = \deg(r) = \deg(s) + \deg(t).$$

This implies that s and t must be constant polynomials, i.e. $s, t \in R$. But r is irreducible in R, thus $s \in R^* = R[x]^*$ or $t \in R^* = R[x]^*$ and we are done.

c. Let $r \mid s \cdot t = \sum_{k=0}^{m+n} \left(\sum_{l=0}^{k} s_l t_{k-l}\right) \cdot x^k$ where $s = \sum_{i=0}^{m} s_i x^i, t = \sum_{i=0}^{n} t_i x^i \in R[x]$ and where we set $s_i = 0 = t_j$ if $i > m$ or $j > n$. Suppose that $r \not| s$ and $r \not| t$. Since $r \in R$ this implies that there are i, j such that $r \not| s_i$ and $r \not| t_j$. Let i_0 respectively j_0 be minimal with the property that $r \not| s_{i_0}$ and $r \not| t_{j_0}$. Since $r \mid s \cdot t$ and r is constant r divides every coefficient of $s \cdot t$, in particular

$$r \mid \sum_{l=0}^{i_0+j_0} s_l \cdot t_{k-l}.$$

But by the choice of i_0 and j_0 we know that r divides every summand except possibly $s_{i_0} \cdot t_{j_0}$, which then implies that r divides this one as well. However, r is prime and must therefore divide s_{i_0} or t_{j_0} in contradiction to the choice of i_0 and j_0. This finishes the proof.

□

1.38 Theorem (Lemma of Gauß)
If R is a UFD, then $R[x]$ is a UFD.

Proof: Let $0 \neq f = \sum_{i=0}^{n} f_i x^i \in R[x] \setminus R[x]^*$ and $d \in \gcd(f_0, \ldots, f_n)$. Since R is a UFD and taking Lemma 1.37 into account there are $q_1, \ldots, q_l \in R$ irreducible in R and hence in $R[x]$ such that

$$d = q_1 \cdots q_l. \tag{1}$$

We define $f_i' = \frac{f_i}{d}$ and $f' = \frac{f}{d} = \sum_{i=0}^{n} f_i' x^i$. Note that then the f_i' have no common divisor, i.e.

$$\gcd(f_0', \ldots, f_n') = R^*.$$

We first of all show that there are irreducible elements $p_1, \ldots, p_k \in R[x]$ such that $f = p_1 \cdots p_k$ by induction on $n = \deg(f) = \deg(f')$. If $n = 0$ then $f = d \in R$ and we are done by (1). Thus we may assume that $n > 0$. In case f' is irreducible, we have $f = d \cdot f' = p_1 \cdots p_k \cdot f'$ is a product of finitely many irreducible polynomials in $R[x]$. It remains to consider the case where f' is not irreducible. In that case $f' = g \cdot h$ where neither $g \in R[x]^*$ nor $h \in R[x]^*$ is a unit. By the degree formula over integral domains we have

$$n = \deg(f) = \deg(g) + \deg(h).$$

Suppose that $\deg(g) = 0$, then $g \in R$ and hence g divides the coefficients of f', i.e. $g \mid f_0', \ldots f_n'$. But since they do not have a common divisor, this implies $g \mid 1$, i.e. $g \in R^* = R[x]^*$, in contradiction to our assumption. Thus $\deg(g) > 0$, and analogously $\deg(h) > 0$, which implies $\deg(g), \deg(h) < n$. By induction g and h do

factorise in a finite product of irreducible elements as well as d does by (1), hence so does $f = d \cdot g \cdot h$.
By Proposition 1.34 it remains to show that each irreducible polynomial $f \in R[x]$ is actually prime. We postpone this to Lemma 3.15, since we need the notion of the quotient field of R which we have not yet introduced. $\square$

1.39 Corollary
If K is a field, then $K[x_1, \ldots, x_n]$ is a UFD.

1.40 Corollary
$R[x]$ is a PID if and only if R is a field.
*In particular, $K[x_1, \ldots, x_n]$ is **not** a PID once $n \geq 2$.*

Proof: If R is a field we have seen in Corollary 1.29 that $R[x]$ is a PID.
For the converse consider the R-algebra homomorphism

$$\varphi : R[x] \to R : f \mapsto f(0).$$

By the Homomorphism Theorem we have $R[x]/\ker(\varphi) \cong R$, and since R is an integral domain this implies that $\ker(\varphi)$ must be a prime ideal. However, $\ker(\varphi)$ is not the zero ideal, since $x \in \ker(\varphi)$, and hence by Proposition 1.30 it is indeed a maximal ideal. Thus $R \cong R[x]/\ker(\varphi)$ is a field. $\square$

1.41 Theorem
*$\mathbb{Z}[\omega] = \{a + b \cdot \omega \mid a, b \in \mathbb{Z}\} \leq \mathbb{C}$, with $\omega = \frac{1+\sqrt{-19}}{2} \in \mathbb{C}$, is a PID, but it is **not** Euclidean.*
The proof of this theorem needs some preparation.

1.42 Proposition
Let R be an ID.
Then R is a PID if and only if there exists a function $\alpha : R \to \mathbb{N}$ such that

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

You may consider $ua - vb$ as a greatest common divisor of a and b, so that the existence of α basically means that the ideal $\langle a, b \rangle$ is principle and generated by a greatest common divisor.

Proof: Let us first assume R is a PID, and hence by Corollary 1.32 it is a UFD. We now define $\alpha : R \to \mathbb{N}$ by

$$\alpha(r) = \begin{cases} 0, & \text{if } r = 0, \\ 1, & \text{if } r \in R^*, \\ 1 + k & \text{if } r = p_1 \cdots p_k \text{ with } p_i \text{ irreducible.} \end{cases}$$

Given $a, b \in R$ with $0 \neq b \not| a$ we choose $g \in \gcd(a, b)$. Then by definition

$$\alpha(0) = 0 < \alpha(g) < \alpha(b),$$

and by Remark 1.36 we have

$$\langle g \rangle = \langle a, b \rangle.$$

This, however, implies that $g = a \cdot u - b \cdot v$ for suitable $u, v \in R$.
Let us now assume that the desired function α exists, and let $0 \neq I \trianglelefteq R$ be given. We may choose $0 \neq b \in I$ with $\alpha(b)$ minimal, and we claim $I = \langle b \rangle$. Suppose there is some $a \in I \setminus \langle b \rangle$, then $b \not| a$ and by assumption there are $u, v \in R$ such that

$$\alpha(0) < \alpha(ua - vb) < \alpha(b).$$

In particular, $0 \neq ua - vb \in I$ in contradiction to the assumption that $\alpha(b)$ is minimal. Thus $I = \langle b \rangle$. $\square$

1.43 Proposition
Let R be a Euclidean ring via $\nu : R\setminus\{0\} \rightarrow \mathbb{N}$, let $0 \neq p \in R\setminus R^*$ with $\nu(p)$ minimal, and let $\pi : R \rightarrow R/\langle p \rangle : a \mapsto \overline{a}$ be the residue map. Then the following statements hold:

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

b. *If $a \in R$, then there are $q, r \in R$ such that $a = q \cdot p + r$ with $r = 0$ or $r \in R^*$.*

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

Proof: Let $a \in R$ be given. Since R is Euclidean there exists $q, r \in R$ such that $a = q \cdot p + r$ with $r = 0$ or $\nu(r) < \nu(p)$. By the choice of p this implies $r = 0$ or $r \in R^*$, which proves b..
Moreover, $\pi(a) = \pi(r) = 0$ or $\pi(a) = \pi(r) \in \pi(R^*) \subseteq K^*$, since units are mapped to units by ring homomorphisms. Since π is surjective we get

$$K = \pi(R) = \{0\} \cup \pi(R^*) \subseteq \{0\} \cup K^* = K,$$

and thus $K = \{0\} \cup K^*$, which implies that $\pi(R^*) = K^*$, that is c., and that K is a field. But then $\langle p \rangle \lhd \cdot R$ and p must be prime element, which finally proves a.. $\square$

Proof of Theorem 1.41 (see [Bru00] **p. 90f.):** For $a + b\omega \in \mathbb{Z}[\omega]$ with $a, b \in \mathbb{Z}$ we define $N : R \rightarrow \mathbb{N}$ by

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

We first of all show that $R^* = \{1, -1\} = \{x \in R \mid N(x) = 1\}$. For this suppose that $1 = x \cdot y$ for $x = a + b\omega, y \in R$. Then

$$1 = |x|^2 \cdot |y|^2$$

where both factors are natural numbers. This implies that

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

and thus $b^2 = 0$ and $\left(a + \frac{b}{2}\right)^2 = 1$, i.e. $b = 0$ and $a \in \{1, -1\}$.

We next claim that 2 **and** 3 **are irreducible in** R. Suppose that $2 = x \cdot y$ for $= a + b\omega, y \in R \setminus R^*$, then

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

and $N(x), N(y) > 1$. Both being natural numbers this implies

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

But then $b^2 = 0$ and hence $b = 0$, which gives $a^2 = 2$ for an integer a. Thus we have derived the desired contradiction, and 2 is irreducible. The proof for 3 works analogously.

Next we show that R **is *not* Euclidean**. Suppose R was Euclidean. Then we may choose $p \in R$ as in Proposition 1.43 and we deduce with the notation from that proposition

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

Since $R/\langle 2\rangle = \left\{\overline{0}, \overline{1}, \overline{\sqrt{-19}}, \overline{1 + \sqrt{-19}}\right\}$ has four elements we know that $p \neq 2$. Thus there are elements $q, r \in R$ such that $2 = q \cdot p + r$ and, since 2 is irreducible, $r \neq 0$, which implies that $r \in R^* = \{1, -1\}$ is a unit. If $r = 1$, then $1 = q \cdot p$ in contradiction to p being prime. If $r = -1$, then $3 = q \cdot p$, and since 3 is irreducible we get $\langle 3\rangle = \langle p\rangle$. However,

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

in contradiction to the fact that K has only 3 elements. This shows that R cannot be Euclidean.

We claim that

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

where the calculations are done in $\mathbb{C}$. Note that actually $\frac{x}{y} \in \mathbb{Q}[\omega]$, that is

$$\exists\, a', b', a, b, q, s \in \mathbb{Z} \text{ with } 0 \leq a < q, 0 \leq b < s, 1 \in \gcd(a, q) \text{ and } 1 \in \gcd(b, s)$$
$$\text{such that } \frac{x}{y} = \left(a' + \frac{a}{q}\right) + \left(b' + \frac{b}{s}\right) \cdot \omega.$$

If we now find $u', v' \in R$ 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

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

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

If $b = 0$, then we are done by $u = 1$ and $v = 0$. Thus we may assume $b \neq 0$.

If $q \not| s$, then $s \cdot a \not\equiv 0 \pmod q$, and there exists $0 < d < q$ and $c \in \mathbb{Z}$ such that $sa = cq + d$. Thus

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

where the right hand side is strictly between 0 and 1. Thus we are done with $u = s$ and $v = c + b\omega$.

If $q \mid s$ and $s > 2$, then, since s and b have no common divisor, there exists an $m \in \mathbb{Z}$ such that $m \cdot b \equiv 1 \pmod s$. Thus

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

for suitable $l, k, a_1, a_2 \in \mathbb{Z}$ such that $\left|\frac{a_1}{a_2}\right| \leq \frac{1}{2}$. Setting $u = m$ and $v = l + k\omega$ we get

$$\begin{aligned}\left|u\cdot\frac{x}{y}-v\right|^2 &= \left|\frac{a_1}{a_2}+\frac{1}{s}\cdot\frac{1+\sqrt{-19}}{2}\right|^2\\ &= \left(\frac{a_1}{a_2}+\frac{1}{2s}\right)^2+\frac{19}{4s^2} = \frac{a_1^2}{a_2^2}+\frac{a_1}{a_2 s}+\frac{20}{4s^2}\\ &\leq \frac{1}{4}+\frac{1}{6}+\frac{20}{36} = \frac{35}{36} < 1,\end{aligned}$$

and we are done.

Finally, if $q \mid s$ and $s = 2$, then $q = s = 2$ and $\frac{x}{y} = \frac{\omega}{2}$ or $\frac{x}{y} = \frac{1+\omega}{2}$. In the first case we set $u = 1 + \omega$ and $v = -2 + \omega$, in the second case we set $u = \omega$ and $v = -2 + \omega$. So, in any case we have

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

and we are done.

We conclude that (2) holds, which implies that $\alpha = N$ is a function as required in Proposition 1.42, and thus R is a PID. □

1.44 Remark

For the following results see [Bru00], Chapter 8–10, and [ScS88], pp. 154ff, p. 168 Exercise 40, p. 167 Exercise 31c. and p. 186 Exercise 23.

a. $K = \mathbb{Q}[x]/\langle f\rangle$ with $\deg(f) = 2$ if and only if $K = \mathbb{Q}\big[\sqrt{d}\big]$ for some squarefree $d \in \mathbb{Z} \setminus \{0, 1\}$. If $f = x^2 + ax + b$, then $d = \frac{a^2}{4} - b$ is its discriminant.

b. If d is such a squarefree number, then $\mathbb{Z}[\omega_d] = \big\{a \in \mathbb{Q}\big[\sqrt{d}\big] \;\big|\, a \text{ is integral over } \mathbb{Z}\big\}$ for

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

c. $\mathbb{Z}[\omega_d]$ is a UFD if and only if it is a PID.

d. If $d \leq -1$, then
   (i) $\mathbb{Z}[\omega_d]$ is a UFD if and only if $d \in \{-1, -2, -3, -7, -11, -19, -43, -67, -163\}$.
   (ii) $\mathbb{Z}[\omega_d]$ is a UFD if and only if $d \in \{-1, -2, -3, -7, -11\}$.

e. $\mathbb{R}[x, y]/\langle x^2 + y^2 + 1\rangle$ is a PID, but not Euclidean.

1.45 Remark

We have seen (Theorem 1.41 and Corollaries 1.39 and 1.40) that

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

and that neither of the converses holds!

References

[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.

Universität Kaiserslautern, Fachbereich Mathematik, Erwin-Schrödinger-Strasse, D – 67663 Kaiserslautern

E-mail address: `keilen@mathematik.uni-kl.de`

URL: `http://www.mathematik.uni-kl.de/~keilen`