# 7 Euclidean domains

A domain $\mathcal{R}$ is called *Euclidean* if there is a *Euclidean norm* $\nu$, that is, a function $\nu\colon R \to \mathbb{N}$, which satisfies

1. $\nu(0) = 0$
2. If $a \mid b$, $b \neq 0$, then $\nu(a) \leq \nu(b)$;
3. for all $a, b \in R$, $b \neq 0$, there exists $q, r \in R$ such that $a = bq + r$ and $\nu(r) < \nu(b)$.

**7.1.** Prove that for any square-free $s \in \mathbb{Z}$, the norm $\nu(a+b\sqrt{s}) = |a^2 - sb^2|$ on the domain $\mathbb{Z}[\sqrt{s}]$ satisfies axioms (1) and (2).

**7.2.** Using the relationship between the modulus in $\mathbb{C}$ (in Czech: absolutní hodnota) and the norm $\nu(a + bi) = |a^2 + b^2| = |a + bi|^2$ of the domain $\mathbb{Z}[\sqrt{i}]$, prove for arbitrary $a, b \in \mathbb{Z}[i]$, $b \neq 0$ and $z := \frac{a}{b} \in \mathbb{C}$

(a) that there exists $q \in \mathbb{Z}[i]$ such that $\mid z - q \mid < 1$,

(b) that $|r| < |b|$ and $\nu(r) < \nu(b)$ if $r := a - bq$ for $q$ from (a),

(c) that $\nu$ is a Euclidean norm, hence the domain $\mathbb{Z}[\sqrt{i}]$ is Euclidean.

**7.3.** Divide with the remainder $\alpha$ by $\beta$ in the domain $\mathbb{Z}[i]$ using the Euclidean norm $\nu(a + bi) = |a^2 + b^2|$. Notice that the algorithm (formulated in 7.2) is not deterministic.

(a) $\alpha = 5 + 7i$, $\beta = 3 - i$,

(b) $\alpha = 3 + 2i$, $\beta = 1 + i$,

*Solutions: (a)* $\alpha = (1 + 3i) \cdot \beta + (-1 - i) = (1 + 2i) \cdot \beta + (2i)$,
*(b)* $\alpha = 2 \cdot \beta + 1 = 3 \cdot \beta + (-i) = (2 - i) \cdot \beta + i = (3 - i) \cdot \beta - 1$

**Euclid's algorithm** (over a Euclidean domain **R**).

- Input: $a, b \in R$, with $\nu(a) \geq \nu(b)$
- Output: $\gcd(a, b)$ and coefficients $u, v \in R$ such that $\gcd(a, b) = u \cdot a + v \cdot b$
  - $a_0 = a, \quad u_0 = 1, \quad v_0 = 0, \quad a_1 = b, \quad u_1 = 0, \quad v_1 = 1$
  - for every $i = 1, 2 \ldots$ do the following:
    let $q, r$ be such that $a_{i-1} = qa_i + r$ and $\nu(r) < \nu(a_i)$. Then set

$$a_{i+1} = r, \quad u_{i+1} = u_{i-1} - qu_i, v_{i+1} = v_{i-1} - qv_i.$$

    If $a_{i+1} = 0$, output $a_i, u_i, v_i$.

**7.4.** Check that the proof of correctness of Euclid's algorithm in $\mathbb{Z}$ works also for the general Euclid's algorithm.

**7.5.** Find the greatest common divisors and the corresponding Bézout's coefficients in $\mathbb{Z}[i]$

(a) $7 + i$ and $5 - 3i$,

(b) $4 + 2i$ and $3 + i$.

*Solutions: (a)* $\gcd(5 - 3i, 7 + i) = -1 - i = 1 \cdot (7 + i) - (1 + i) \cdot (5 - 3i)$,
*(b)* $\gcd(3 + i, 4 + 2i) = 1 + i = 1 \cdot (4 + 2i) - 1 \cdot (3 + i)$

**7.6.** Calculate the irreducible decompositions of 2, 3, 5 and 6 in the domain $\mathbb{Z}[i]$.

*Solutions:* $2 = (1 + i)(1 - i)$, 3, $5 = (1 + 2i)(1 - 2i)$, $6 = 3(1 + i)(1 - i)$

**7.7.**$^\star$ Show that the following subdomains of $\mathbb{C}$ are Euclidean:

(a) $\mathbb{Z}[\sqrt{2}i]$ with the Euclidean norm $\nu(a + b\sqrt{2}i) = |a^2 + 2b^2|$,

(b) $\mathbb{Z}[\sqrt{2}]$ with the Euclidean norm $\nu(a + b\sqrt{2}) = |a^2 - 2b^2|$,

(c) $\mathbb{Z}[\sqrt{3}]$ with the Euclidean norm $\nu(a + b\sqrt{3}) = |a^2 - 3b^2|$.

**7.8.**$^\star$ Using the Euclidean norm from 7.7

(a) divide with the remainder 4 by $1 - \sqrt{2}i$ in $\mathbb{Z}[\sqrt{2}i]$,

(b) divide with the remainder $3 + \sqrt{2}i$ by $3 + \sqrt{2}i$ in $\mathbb{Z}[\sqrt{2}i]$,

(c) $\gcd(6 - 3\sqrt{3}, 3 + \sqrt{3})$ in $\mathbb{Z}[\sqrt{3}]$

*Solutions: (a)* $4 = (1 + \sqrt{2}i)(1 - \sqrt{2}i) + 1$, *(b)* $(1 + 4\sqrt{2}i) = (3 + \sqrt{2}i) \cdot (1 + \sqrt{2}i) + 0$,
*(c)* $\gcd(6 - 3\sqrt{3}, 3 + \sqrt{3}) = \sqrt{3}$.