1.B PIDs and Euclidean Domains

In this section we study divisibility properties in PIDs. This study is modelled on the two most important examples: the ring of integers $\mathbb{Z}$ and the polynomial rings $K[X]$, where K is a field.

Recall that an integral domain A is called a PID (principal ideal domain) if every ideal $\mathfrak{a}$ in A is principal i.e. generated by a single element $a \in \mathfrak{a}$, i.e. $\mathfrak{a} = Aa$.

1.B.1 Theorem Every PID is factorial.

Proof Imediate from 1.A.13, 1.A.12 and the following lemma:

1.B.2 Lemma Let A be a PID and let $\pi \in A$ be an irreducible element. Then $A\pi$ is a maximal ideal in A

Proof Since π is irreducible, $\pi \notin A^\times$, i.e. $A\pi \neq A$. Let $\mathfrak{b}$ be an ideal in A with $A\pi \subseteq \mathfrak{b}$. Then, since A is a PID, $\mathfrak{b} = Ab$ for some $b \in A$. Further, since $\cdot \in Ab$ $\iota = cb$ for some $c \in A$. Now, since π is irreducible, either $c \in A^\times$ or $b \in A^\times$, i.e. either $A\pi = Ab = \mathfrak{b}$ or $Ab = \mathfrak{b} = A$.

1.B.3 Corollary Every polynomial ring $K[X]$ over a field K is factorial.

Proof $K[X]$ is a PID (see

The method of proof to show that the ring of integers $\mathbb{Z}$ and a polynomial ring $K[X]$ over a field is a PID can also be applied in other cases and leads us to the following definition:

1.B.4 Definition Let A be an integral domain. An Euclidean function on A is a map

$$\nu : A \setminus \{0\} \longrightarrow \mathbb{N}$$

with the following property:

for every two elements $a, b \in A$ with $b \neq 0$, there exist elements q and $r \in A$ such that

$$a = qb + r \quad \text{and either } r = 0 \text{ or } (r \neq 0 \text{ and } \nu(r) < \nu(b)).$$

The element q is called the quotient and the element r is called the remainder of the division.

An integral domain A with an Euclidean function is called Euclidean or an Euclidean domain.

1.B.5 Examples

(1) The ring of integers $\mathbb{Z}$ together with the absolute value function $|-|: \mathbb{Z} \longrightarrow \mathbb{N}$, $a \longmapsto |a|$ is an Euclidean domain.

(2) Let $K[X]$ be a polynomial ring over a field K. Then $K[X]$ together with the degree function $\deg: K[X] \setminus \{0\} \to \mathbb{N}$, $f \longmapsto \deg f$ is an Euclidean domain.

(3) For $m \in \{-2, -1, 2, 3\}$, the ring of quadratic integers $\mathbb{Z}[\sqrt{m}]$ together with the norm-function $\eta: \mathbb{Z}[\sqrt{m}] \to \mathbb{N}$, $\eta(a+b\sqrt{m}) = |a^2 - b^2 m|$ is an Euclidean domain (see

The first implication of an Euclidean algorithm for the integral domain A is that every ideal in A is principal.

(with an Euclidean function)

1.B.6 Theorem Every Euclidean domain A is a PID. More precisely, if $0 \neq \mathfrak{a}$ is an ideal in A, then $\mathfrak{a} = Ab$, where $0 \neq b \in \mathfrak{a}$ is an element with $\nu(b) = \mathrm{Min}(\mathfrak{a} \setminus \{0\})$. In particular, every Euclidean domain is a factorial domain.

Proof Let $a \in \mathfrak{a}$ and let $q, r \in A$ be such that $a = qb + r$ with either $r = 0$ or $r \neq 0$ and $\nu(r) < \nu(b)$. Then, since $r = qb - a \in \mathfrak{a}$, $r = 0$ by the minimality of $\nu(b)$. Therefore $a = qb$; this proves that $\mathfrak{a} = Ab$.

1.B.7 Remark Note that the Euclidean functions given in examples 1.B. give more information on the divisibility, since they are multiplicative. Many authors assume that in the definition of ~~an~~ Euclidean function ν respect multiplication, not as strongly as in the above examples: , but somewhat weaker, namely: for non-zero elements $a, b \in A$, $\nu(ab) \geq \nu(a)$. However, even this is not really necessary, see for example [Claus, H.J], Crelle Journal, 1954 and [Samuel, P.] About Euclidean Rings, Journal of Algebra, 19 (1971), 282-30

1.B.8 Corollary The ring of integers $\mathbb{Z}$ and a polynomial ring over a field K are PIDs

1.B.9 (one of the fundamental consequence of)

In an Euclidean domain A the Euclidean algorithm (is that it) gives an algorithmic procedure for computing the gcd of two elements $a, b \in A$:

By successive "divisions" we can write:

$a_0 := a, \quad a_1 := b$

$$a_0 = q_0 a_1 + a_2$$
$$a_1 = q_1 a_2 + a_3$$
$$\vdots$$
$$a_{n-1} = q_{n-1} a_n + a_{n+1}$$
$$a_n = q_n a_{n+1} \qquad i \geq 2$$

with $a_0, \cdots, a_{n+1} \in A$, $a_i \neq 0$ and $\upsilon(a_i) < \upsilon(a_{i-1})$ for $i \geq 2$

(Note that such a sequence $a_1, a_2, \cdots, a_{n+1}$ of non-zero elements in A exists, since $\upsilon(a_1) > \upsilon(a_2) > \cdots > \upsilon(a_{n+1})$ is a decreasing sequence of natural numbers and hence cannot continue indefinitely. Note also that there is no guarantee that these elements are unique). Then

$$\gcd(a, b) = \gcd(a_0, a_1) = a_{n+1}$$

For this check that $\gcd(a_i, a_{i+1}) = \gcd(a_{i+1}, a_{i+2})$ for all $i = 0, \cdots, n-2$, using (the equation) $a_i = q_i a_{i+1} + a_{i+2}$.

The divisibility properties an integral domain A can be transfered to the ordered set $(\mathbb{N}, \leq)$ by using a norm-function:

1.B.10 Definition Let A bean integral domain. A map $\eta: A \longrightarrow \mathbb{N}$ is called a norm-function on A if (1) $\eta(a) = 0 \Longleftrightarrow a = 0$ and (2) η is multiplicative, i.e $\eta(ab) = \eta(a)\eta(b)$ for all $a, b \in A$.

We list simple properties of norm-functions:

1.B.11 Properties of Norm-functions: Let A be an integral domain and let $\eta: A \longrightarrow \mathbb{N}$ be a norm-function on A. Then: for $a, b \in A$,

(1) If $a \mid b$ and $b \neq 0$, then $1 \leq \eta(a) \leq \eta(b)$.

(2) If a is associate of b, then $\eta(a) = \eta(b)$.

(3) If a is a unit in A, then $\eta(a) = 1$.

Proof (1) If $a \mid b$ and $b \neq 0$, then there exists $c \in A$ with $ac = b \neq 0$ and hence $\eta(a)\eta(c) = \eta(ac) = \eta(b) \neq 0$. Therefore $\eta(a) \mid \eta(b)$. Further, since $\eta(b) \neq 0$, we have $1 \leq \eta(a) \leq \eta(b)$.

(2) If $b = 0$ then $a = 0$ and the assertion is clear. Therefore assume $b \neq 0$, then $a \mid b$ and $b \mid a$ and so (by (1)) $1 \leq \eta(a) \leq \eta(b)$ and $1 \leq \eta(b) \leq \eta(a)$. Therefore $\eta(a) = \eta(b)$.

(3) Since $1 \cdot 1 = 1$, we have $\eta(1)\eta(1) = \eta(1) \neq 0$ and hence $\eta(1) = 1$. Now, if $a \in A^{\times}$, then a is an associate of 1 and so $\eta(a) = \eta(1) = 1$ by (2).

1.B.12 Examples

(1) On every integral domain A, the trivial function

$\eta : A \longrightarrow \mathbb{N}$, $\eta(0)=0$ and $\eta(a)=1$ for all $a \in A \setminus \{0\}$ is a norm-function called the trivial norm function on

(2) The absolute value on $\mathbb{Z}$:

$$|-|: \mathbb{Z} \longrightarrow \mathbb{N}, \quad |a| := \begin{cases} a, & \text{if } a \geq 0, \\ -a, & \text{if } a < 0 \end{cases}$$

is a norm-function on $\mathbb{Z}$.

(3) On the polynomial ring $A[X]$ over an integral domain A, the function $A[X] \longrightarrow \mathbb{N}$ defined by $\eta(f) = \begin{cases} 0, & \text{if } f=0, \\ 2^{\deg f}, & \text{if } f \neq 0, \end{cases}$ is a norm function on $A[X]$ (for $f, g \in A[X]$, $f \neq 0$, $g \neq 0$, the degree formula $\deg(fg) = \deg(f) + \deg(g)$ shows that $\eta(fg) = \eta(f)\eta(g)$.

(4) Let $m \in \mathbb{Z}$ be an integer which is not a square in $\mathbb{Z}$ and let $\mathbb{Z}[\sqrt{m}]$ be a ring of quadratic integers. Then the function $\eta : \mathbb{Z}[\sqrt{m}] \longrightarrow \mathbb{N}$ defined by $x = a + b\sqrt{m} \longmapsto |x \cdot \bar{x}| = |(a+b\sqrt{m})(a-b\sqrt{m})| = |a^2 - b^2 m|$ is a norm-function on $\mathbb{Z}[\sqrt{m}]$. (Immediate from the fact that the norm $N(x) := x\bar{x}$ is multiplicative).

1.B.13 Definition A norm-function $\eta : A \longrightarrow \mathbb{N}$ on an integral domain is called monotone if for a proper divisor a of an element $b \neq 0$, we have $\eta(a) < \eta(b)$.

1.B.14 Lemma A norm-function $\eta : A \longrightarrow \mathbb{N}$ on an integral domain is monotone if and only if every element $e \in A$ with $\eta(e) = 1$ is a unit in A.

Proof ($\Rightarrow$) Let $e \in A$ be such that $\eta(e) = 1$. Since $1 \mid e$, by 1.B. $1 \leq \eta(1) \leq \eta(e) = 1$, i.e. $\eta(1) = \eta(e)$.
Therefore, since η is monotone, 1 and e are associates, i.e. e is a unit in A.
($\Leftarrow$) Suppose that $a, b \in A$ and $a \| b$. Then there exist $c \in A$, $c \neq 0$, $c \notin A^\times$ with $b = ac$. Therefore $\eta(c) > 1$ by assumption (since $c \notin A^\times$) and $\eta(a) \cdot \eta(c) = \eta(ac) = \eta(b) \neq 0$ and hence $\eta(a) < \eta(b)$. This proves that η is monotone.

1.B.15 Examples

(1) The trivial norm-function on $\mathbb{Z}$ is not monotone
(2) The absolute value function on $\mathbb{Z}$ is monotone, since $|e| = 1 \Leftrightarrow e = \pm 1$; therefore $e \in \mathbb{Z}^\times = \{\pm 1\}$.
(3) Let K be a field. Then the degree-norm-functio $\eta(f) = 2^{\deg f}$ on the polynomial ring $K[X]$ over K is monotone, since $\eta(f) = 2^{\deg f} = 1 \Leftrightarrow \deg f = 0$, i.e. $f \in K^\times = K[X]^\times$.
(4) On the ring of quadratic integers $\mathbb{Z}[\sqrt{m}]$, where $m \in \mathbb{Z}$ is not square free. Then the norm-function $\eta(x) = |x \cdot \bar{x}|$ is monotone, since $\eta(x) = 1 \Leftrightarrow x\bar{x} = \pm 1$, i.e. x is a unit in $\mathbb{Z}[\sqrt{m}]$ (with inverse $\pm\bar{x} \in \mathbb{Z}[\sqrt{m}]$).
In particular, the unit group

$$\mathbb{Z}[\sqrt{m}]^\times = \left\{ a + b\sqrt{m} \in \mathbb{Z}[\sqrt{m}] \;\middle|\; a^2 - b^2 m = \pm 1 \right\}.$$

Further in the imaginary quadratic case (i.e. $m \leq -1$):
$\mathbb{Z}[\sqrt{m}] = \{\pm 1\}$ if $m < -1$ and $\mathbb{Z}[\sqrt{-1}] = \{\pm 1, \pm i\}$

(Remark In the real quadratic case (i.e. $m > 1$) the description of the unit group of $\mathbb{Z}[\sqrt{m}]$ is much more difficult)

1.B.16 Proposition Let $m \in \mathbb{Z}$, $m \neq 1$, be a square free integer. Suppose that $\eta(\alpha+\beta\sqrt{m}) = |\alpha^2 - \beta^2 m| < 1$ for all $\alpha, \beta \in \mathbb{Q}$ with $|\alpha| \leq \frac{1}{2}$, $|\beta| \leq \frac{1}{2}$. Then the norm-function $\eta: \mathbb{Z}[\sqrt{m}] \longrightarrow \mathbb{N}$, $a+b\sqrt{m} \longmapsto \eta(a+b\sqrt{m}) = a^2 - b^2 m$, $a, b \in \mathbb{Z}$, is an Euclidean function on $\mathbb{Z}[\sqrt{m}]$.

Proof Let $x, y \in \mathbb{Z}[\sqrt{m}]$ be any two non-zero elements with $y \nmid x$ and $\eta(x) \geq \eta(y)$. Then we are looking for two elements $q, r \in \mathbb{Z}[\sqrt{m}]$, $r \neq 0$ with $x = qy + r$ and $\eta(r) < \eta(x)$.

The trick is to calculate in the quotient field $\mathbb{Q}(\sqrt{m})$ of $\mathbb{Z}[\sqrt{m}]$: $x/y \in \mathbb{Q}(\sqrt{m})$, i.e. $\frac{x}{y} = \alpha' + \beta'\sqrt{m}$, $\alpha', \beta' \in \mathbb{Q}$. Write $\alpha' = a + \alpha$, $\beta' = b + \beta$ with $a, b \in \mathbb{Z}$, $\alpha, \beta \in \mathbb{Q}$ and $|\alpha| \leq \frac{1}{2}$, $|\beta| \leq \frac{1}{2}$. Put $q := a + b\sqrt{m}$, $r = x - qy \in \mathbb{Z}[\sqrt{m}]$. $\xi = \alpha + \beta\sqrt{m}$. Then $r = \xi y \in \mathbb{Z}[\sqrt{m}]$, $r \neq 0$, since $y \nmid x$. Further, $N(r) = N(\xi y) = N(\xi)\,N(y)$ and $|N(\xi)| = |\alpha^2 - \beta^2 m| <$ by assumption (since $|\alpha| \leq \frac{1}{2}$ and $|\beta| \leq \frac{1}{2}$). Therefore, since $y \neq 0$, $N(y) \neq 0$ and $\eta(r) = |N(r)| = |N(\xi)|\,|N(y)| < |N(y)| = \eta(y) \leq \eta(x)$ by assumption.

1.B.17 Corollary For $m \in \{-2, -1, 2, 3\}$ the norm-function $\eta: \mathbb{Z}[\sqrt{m}] \longrightarrow \mathbb{N}$, $x = a + b\sqrt{m} \longmapsto \eta(x) = |a^2 - b^2 m|$ is an Euclidean function on $\mathbb{Z}[\sqrt{m}]$. In particular, $\mathbb{Z}[\sqrt{m}]$ is an Euclidean domain for $m = -2, -1, 2, 3$.

Proof Let $\alpha, \beta \in \mathbb{Q}$ be such that $|\alpha| \leq \frac{1}{2}$ and $|\beta| \leq \frac{1}{2}$. Then $\alpha^2 \leq \frac{1}{4}$ and $\beta^2 \leq \frac{1}{4}$ and hence $|\alpha^2 - \beta^2 m| \leq$

$3/4 < 1$, if $m = -2$,

$1/2 < 1$, if $m = -1$,

$1/2 < 1$, if $m = 2$,

$3/4 < 1$, if $m = 3$.

Therefore the assumptions in 1.B. are satisfied and hence η is an Euclidean function on $\mathbb{Z}[\sqrt{m}]$.

1.B.18 Example Let $m \in \mathbb{Z}$ be such that either $m \leq -3$ or $m \equiv 1 \pmod 4$. Then 2 is a irreducible element in $\mathbb{Z}[\sqrt{m}]$. In particular, $\mathbb{Z}[\sqrt{m}]$ is neith~~er~~ factorial domain nor a PID. (2 is not prime in any $\mathbb{Z}[\sqrt{m}]$, 1-A.9

Proof Suppose that $x = a + b\sqrt{m} \in \mathbb{Z}[\sqrt{m}]$ is a proper divisor of 2 in $\mathbb{Z}[\sqrt{m}]$. Then $x \notin \mathbb{Z}[\sqrt{m}]^\times$ and $\eta(x) = |a^2 - b^2 m|$ is a proper divisor of $\eta(2) = 4$. Therefore $\eta(x) = 2$, since $\eta(x) \in \mathbb{N}$, i.e. $2 = \eta(x) = |a^2 - b^2 m| = \pm(a^2 - b^2$

Case: $m \equiv 1 \pmod 4$, i.e. $m = 4k+1$, $k \in \mathbb{Z}$: In this case

$$a^2 - b^2(4k+1) = \pm 2 \iff a^2 - b^2 = 2(2kb^2 \pm 1) \equiv \pm 2 \pmod 4$$

In particular, either both a and b are even or both a and b are odd. If $a = 2s$, $b = 2t$ with $s, t \in \mathbb{Z}$, then $a^2 - b^2 = 4(s^2 - t^2) \equiv 0 \pmod 4$. If $a = 2u+1$, $b = 2v+1$ with $u, v \in \mathbb{Z}$, then $a^2 - b^2 = 4(u^2 + u - v^2 - v) \equiv 0 \pmod 4$. In either case we lead to a contradiction.

Case: $m \leq -3$: In this case $2 = a^2 + b^2|m|$ which is a contradiction, since $a, b \in \mathbb{Z}$ and $|m| \geq 3$.

1.B.19 Example (Dedekind) The integral domain $\mathbb{Z}[\sqrt{-5}]$ has the following properties:

(a) $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$

(b) The elements $2, 3, 1+\sqrt{-5}, 1-\sqrt{-5}$ are irreducible in $\mathbb{Z}[\sqrt{-5}]$.

(c) 2 does not divide either $1+\sqrt{-5}$ or $1-\sqrt{-5}$.
In particular, 2 is neither associate of $1+\sqrt{-5}$ nor of $1-\sqrt{-5}$

(d) 2 is not a prime element in $\mathbb{Z}[\sqrt{-5}]$.

Proof (a) Immediate.

(b) For $x = a+b\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$, we have $N(x) = a^2+5b^2$
Therefore $N(2)=4$, $N(3)=9$, $N(1+\sqrt{-5}) = 6 = N(1-\sqrt{-5})$.
In particular, $2, 3, 1+\sqrt{-5}, 1-\sqrt{-5}$ are non-units in $\mathbb{Z}[\sqrt{-m}$
If x is a proper divisor of any one of $2, 3, 1+\sqrt{-5}$ or $1-\sqrt{-5}$, then $N(x)$ is a proper divisor (either) of $4, 9, 6$ and hence if $x=a+b\sqrt{-5}$ be either 2 or 3, but this is not possible, since (the equation) $a^2+5b^2=2$ and $a^2+5b^2=3$ have no solution with $a, b \in \mathbb{Z}$

(c) If $2 \mid 1+\sqrt{-5}$ or $2 \mid 1-\sqrt{-5}$, then $4 = N(2) \mid N(1 \pm \sqrt{-5}) = 6$ o
Which is absurd.

(d) $2 \mid 6 = (1+\sqrt{-5})(1-\sqrt{-5})$, but neither $2 \mid 1+\sqrt{-5}$ nor $2 \mid 1-\sqrt{-5}$ by (c).