Euclidean domains in Lean

Moritz Hlavaty, Julian Kornweibel

July 22, 2024

1 PIDs

1.1 Definition: Ring

A **ring** is a tuple $(R,\ 0,\ 1,\ +,\ \cdot)$ of a set R with elements $0, 1 \in R$ and two binary operators $+,\ \cdot : R \times R \to R$, for which the following holds true:

- $(R,\ 0,\ +)$ is an abelian group
- $\cdot$ is associative, meaning $\forall r, s, t \in R:\ (r \cdot s) \cdot t = r \cdot (s \cdot t)$
- 1 is neutral element for $\cdot$, meaning $\forall r \in R:\ 1 \cdot r = r \cdot 1 = r$
- The distributive properties hold true for $+$ and $\cdot$:
  $\forall v, s, t \in R : (r + s) \cdot t = r \cdot t + s \cdot t$ and $r \cdot (s + t) = r \cdot s + r \cdot t$

A ring is called commutative ring $\Leftrightarrow \forall r, s \in R : r \cdot s = s \cdot r$

1.1.1 Comment to used convention

In the following parts we will write the additive inverse r^{-1} of $r \in R$ as $-r$. $r + r^{-1} = r + (-r) = 0$

1.2 Definition: integral domain

An **integral domain** is a nonzero ring R, for which the following property holds true: $\forall r, s \in R \backslash \{0\} : r \cdot s \neq 0$

1.3 Definition: ideal

An **left ideal** is a subset $I \subset R$ with R being a Ring, such that:

- $0 \in I$
- $\forall r, s \in I : r + s \in I$
- $\forall r \in R,\ \forall s \in I : r \cdot s \in I$

An **right ideal** is a subset $I \subset R$, for which all properties above are true, with the last one being modified to:

- $\forall r \in R,\ \forall s \in I : s \cdot r \in I$

If both the orignial and the modified porperty hold true for an ideal I it is called a two-sided ideal.
If R is a commutative Ring we just call I an ideal because $r \cdot s = s \cdot r,\ \forall r, s \in R$

1.4 Definition: principle ideal

A **principal ideal** is an Ideal I over a commutative Ring R, such that:
$\exists a \in I : I = (a) := R \cdot a := \{r \cdot a |\ r \in R\}$

1.5 Definition: principle ideal domain

A **principal ideal domain** (PID) is a Ring R with the following properties:

- R is a integral domain
- every ideal I of R is a principal ideal

1.6 Theorem: fields are pid's

Let K be a Field. It suffices to show that $I = (0)$ and $J = (1)$ are the only ideals of K and therefor every ideal is a principal ideal.
Let $I = \{0\} \Rightarrow 0 \in I$
And therefor I is a principal ideal.
Let $a \in K \Rightarrow \exists a^{-1}$ with $a^{-1} \cdot a = 1$
$\Rightarrow \forall a \in K : a \in (1) = J$
And therefor (0) and (1) are the only Ideals of any Field K and both are prim ideals.

2 Euclidean Domains

2.1 Definition: euclidean function

A **euclidean function** is a function $\beta : R \backslash \{0\} \rightarrow \mathbb{N}_0$ with the following porperty: $\forall x, y \in R$ with $y \neq 0$ $\exists q, r \in R$ such that $x = q \cdot y + r$ and $(r = 0 \vee \beta(r) < \beta(y))$

2.2 Definition: euclidean domain

A **euclidean domain** is an integral domain with a euclidean function.

2.3 Theorem: fields are euclidean domains

Let K be a field. K is an PID and therefor an integral domain. Define a function $\beta : K \backslash \{0\} \rightarrow \mathbb{N}_0,\ x \mapsto \beta(x) := c$ for any $c \in K$. Because K is a field $\forall x, y \in K\ \exists q \in K : q = x * y^{-1} \Rightarrow x = qy + r = x * y^{-1} * y + r = x + r = x$ with $r = 0\ \forall x, y \in K$.

2.3 Theorem: euclidean domains are PID's

Let R be an euclidean domain. $\Rightarrow \exists \beta : R \backslash \{0\} \rightarrow \mathbb{N}_0$ Let $I \subset R$ be an ideal.
If $I = 0$ then $I = \{0\} = R \cdot 0$
Let $I \neq 0$
Let $a \in I \backslash \{0\}$ such that $\beta(a) = \min\{\beta(b) | b \in I \backslash \{0\}\}$
Let $b \in I$
Write $b = aq + r$ where either $r = 0$ or $\beta(r) < \beta(a)$
Then $r = a - dq$ and therefor $r \in I$
Suppose $r \neq 0$
$\Rightarrow \beta(r) < \beta(a)$ which is a contradiction to $\beta(a)$ is minimal
$\Rightarrow r = 0 \Rightarrow b = aq$
And therefor I is a prime Ideal.

2.4 Theorem: $\mathbb{Z}$ is an euclidean domain

$\mathbb{Z}$ is an Integral Domain. Define a function $\beta : \mathbb{Z} \backslash \{0\} \rightarrow \mathbb{N}_0,\ x \mapsto \beta(x) := |x|$.
Let $x, y \in \mathbb{Z} \backslash \{0\}$ There are two options $|x| < |y| \vee |x| \geq |y|$
1. $|x| < |y|$
Let $r = x \wedge q = 0$
$\Rightarrow x = 0 * y + x = x$ and $|r| = |x| < |y|$
2. $|x| \geq |y|$
2.1 $y > 0$
We find $q \in \mathbb{Z} : x \geq q * y \wedge x < (q + 1) * y$
2.2 $y < 0$
We find $-q \in \mathbb{Z} : x \geq q * y \wedge x < (q + 1) * y$
Let $r := x - q * y$
$\Rightarrow x = q*y+r = q*y+x-q*y = x$ and $|r| = |x-q*y| < |(q+1)*y-q*y| = |y|$
$\mathbb{Z}$ is a euclidean domain

2.5 Theorem: polynomial rings over fields are euclidean domains

The polynomial ring $K[x]$ over any field is a integral domain. Define a function $\beta : \mathbb{K}[x]\backslash\{0\} \to \mathbb{N}_0,\ f \mapsto \beta(f) := \deg(f)$ with $\deg(f)$ being the degree of f.
Let $f, g \in \mathbb{K}[x]\backslash\{0\}$
There are two options $\deg(f) < \deg(g) \vee \deg(f) \geq \deg(g)$
1: $\deg(f) < \deg(g)$
Let $r = f \wedge q = 0$
$\Rightarrow f = 0 * d + f = f$ and $\deg(r) = \deg(f) < \deg(g)$
2. $\deg(f) \geq \deg(g)$
Let:
$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_mx^m$
$g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_nx^n$
We can subtract from f a suitable multiple of g so as to eliminate the highest term in f:
$f(x) - g(x) \cdot a_mb_nx^{m-n} = p(x)$
where $p(x)$ is some polynomial whose degree is less than that of f.
If $p(X)$ still has degree higher than that of g, we do the same thing again.
Eventually we reach:
$f(x) - g(x) \cdot (a_mb_nx^{m-n} + \cdots) = r(X)$
where either $r = 0$
or r has degree that is less than $\deg(d)$.

2.6 Theorem: the Polynomial ring over $\mathbb{Z}$ is not an euclidean domain

Utilising $2.3 Theorem$, the proof is reduced to showing that $\mathbb{Z}[X]$ is not a PID, and therefor that there exists an Ideal $I \subset \mathbb{Z}[X]$ that is not principal.
Let's assume $I := (2, x) \subset \mathbb{Z}[X]$ to be a principal Ideal.
$\Rightarrow I = (f(x)) = \{g(x) \cdot f(x) | g(x) \in \mathbb{Z}[X]\}$
Since $2 \in I$ and $x \in I$ there must exist $g_1(x), g_2(x) \in I$ such that:
$2 = g_1(x) \cdot f(x)$ and $x = g_2(x) \cdot f(x)$
$\Rightarrow f(x)$ must therefore divide 2 and x.
If $f(x)$ is a constant polynomial, say $f(x) = d$ for some integer d, then d must divide both 2 and x. Since d divides 2, d must be ± 1 or ± 2. However, d cannot divide x since x is not a constant.
If $f(x)$ is a non-constant polynomial, consider its degree. If $deg(f(x)) > 0$, then $f(x)$ cannot divide the constant 2 because a polynomial of degree greater than zero cannot divide a non-zero constant.
$\Rightarrow$ No polynomial f(x) $\in mathbbZ[X]$ is a generator for the ideal $I = (2, x)$.
$\Rightarrow I$ cannot be a principal ideal.
Therefore, $mathbbZ[X]$ contains an ideal that is not principal.
$\Rightarrow mathbbZ[X]$ is not a PID.