date: wednesday, march 20, 2024

Euclidean Domains and Factoring in $D[x]$

A Euclidean domain is a domain that has a division algorithm.

Def^{n}: A domain D is a Euclidean domain if there is a valuation $v: D\setminus\{0\} \to \mathbb{N}$ such that

① $v(a) \le v(ab)$ for all $a,b \ne 0$

② for all $a,b \in D$, $b \ne 0$, there exists q and r such that $a = bq + r$ with $r=0$ or $v(r) < v(b)$.

eg. If $D = \mathbb{Z}$, we use $v: \mathbb{Z}\setminus\{0\} \to \mathbb{N}$

$$a \mapsto |a|.$$

eg. If $D = F[x]$, we use $v: D\setminus\{0\} \to \mathbb{N}$ by

$$p(x) \mapsto \deg p(x).$$

eg. $\mathbb{Z}[i] = \{a+bi \mid a,b \in \mathbb{Z}\}$, this a ring with "standard" multiplication and addition.

Define $v: (\mathbb{Z}[x]\setminus\{0\}) \to \mathbb{N}$

$$a+bi \mapsto a^2+b^2$$

Claim: This v makes $\mathbb{Z}[i]$ an Euclidean Domain

Check the properties: Let $x = a+bi$ and $y = c+di$

Then,

$$xy = (a+bi)(c+di) = (ac-bd)+(ad+bc)i$$

So,

$$v(xy) = (ac-bd)^2 + (ad+bc)^2 = (ac)^2 + (bd)^2 + (ad)^2 + (bc)^2$$

Note,

$$v(x)v(y) = (a^2+b^2)(c^2+d^2) = (ac)^2 + (bd)^2 + (ad)^2 + (bc)^2$$

So have $v(xy) = v(x)v(y)$.

But then,

$$① \; v(x) \le v(x)v(y) = v(xy)$$

is true.

For ②, let $z = a+bi$ and $w = c+di$ with $w \ne 0$.

Viewed as elements of $\mathbb{Q}(i)=\{p+qi \mid p,q\in\mathbb{Q}\}$,

$$\frac{z}{w}=\frac{a+bi}{c+di}=\frac{(a+bi)(c-di)}{(c+di)(c-di)}=\frac{(ac+bd)+(bc-ad)i}{c^2+d^2}$$

Write

$$\frac{ac+bd}{c^2+d^2}=m_1+\frac{n_1}{c^2+d^2} \quad \text{and} \quad \left|\frac{n_1}{c^2+d^2}\right|\leq\frac{1}{2}.$$

m_1: closest integer to $\frac{ac+bd}{c^2+d^2}$

Also,

$$\frac{bc-ad}{c^2+d^2}=m_2+\frac{n_2}{c^2+d^2} \quad \text{and} \quad \left|\frac{n_2}{c^2+d^2}\right|\leq\frac{1}{2}.$$

m_2: integer

So,

$$\frac{z}{w}=(m_1+m_2)+\frac{n_1+n_2 i}{c^2+d^2}.$$

So,

$$z=\frac{z}{w}\cdot w=(m_1+n_2 i)(c+di)+\left(\frac{n_1+n_2 i}{c^2+d^2}\right)(c+di)=wq+r$$

Note, $z, wq\in\mathbb{Z}[i]$, so $z-wq=r\in\mathbb{Z}[i]$.

Then,

$$\begin{aligned}
v(r)&=v\left(\frac{(n_1+n_2 i)}{c^2+d^2}(c+di)\right)\\
&=v(c+di)\,v\left(\frac{n_1+n_2 i}{c^2+d^2}\right)\\
&=v(c+di)\left[\left(\frac{n_1}{c^2+d^2}\right)^2+\left(\frac{n_2}{c^2+d^2}\right)^2\right]\\
&\leq v(c+di)\left(\frac{1}{4}+\frac{1}{4}\right)\\
&=\frac{1}{2}v(c+di)\\
&<v(c+di).
\end{aligned}$$

Theorem: Every Euclidean Domain is a PID.

<u>Proof</u>

Let D be an Euclidean Domain. Let $I\subseteq D$ be an ideal. If $I=\{0\}$, then $I=\langle 0\rangle$. Suppose $I\neq\{0\}$. Let $a\in I$ with $v(a)\leq v(b)$ for all other $b\in I$.

Claim: $I=\langle a\rangle$

Proof: Since $a\in I$, $\langle a\rangle\subseteq I$. Let $b\in I$. By division algorithm,

$$b=aq+r \text{ with } r=0 \text{ or } v(r)<v(a).$$

If $r \neq 0$, then $r = b - aq \in I$ and then $v(r) < v(a)$ gives a contradiction to choice of a.

So $r = 0$, thus $I = \langle a \rangle$. $\square$

Corollary: Every Euclidean Domain is a UFD.

Note: Proving a domain is not Euclidean is difficult.

eg. $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right] = \left\{a + b\left(\frac{1+\sqrt{-19}}{2}\right) \mid a, b \in \mathbb{Z}\right\}$

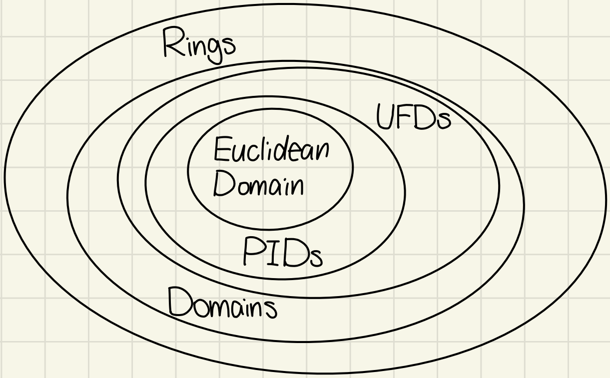
Idea: Suppose there is a valuation $v : D \setminus \{0\} \to \mathbb{N}$. Need to check only units in the ring are ± 1. So, take $a \in D \setminus \{0\}$ with $v(a)$ as small as possible. For any $b \in D$, we have $b = aq + r$ with $r = 0$ or $v(r) < v(a)$. But for units, $v(1) = v(-1) < v(a)$, $v(1) \leq v(1 \cdot a)$. Only three choices for $r = 0, 1, -1$. So

$$D/\langle a \rangle \simeq \mathbb{Z}_2 \text{ or } \mathbb{Z}_3.$$

In D, $x^2 + x + 5$ has roots $x = \frac{-1 \pm \sqrt{-19}}{2}$.
But, $x^2 + x + 5$ has no roots in $\mathbb{Z}_2$ or $\mathbb{Z}_3$.
So

$$D/\langle a \rangle \not\simeq \mathbb{Z}_2 \text{ or } D/\langle a \rangle \not\simeq \mathbb{Z}_3.$$

A contradiction.



Main Theorem: If D is a UFD, then $D[x]$ is a UFD.

Corollary: If D is a UFD, then $D[x_1, \ldots, x_n]$ is a UFD.
Special class $\mathbb{C}[x_1, \ldots, x_n]$.