Last time:

- A Euclidean function is

$$d: R \setminus \{0\} \longrightarrow \mathbb{Z}_{\geq 0}$$

satisfying

(a) $d(a \cdot b) \geq d(a)$ for any nonzero $a, b \in R$

(b) For any $a, b \in R$ $b \neq 0$, there exist $q, r \in R$ satisfying
$$a = b \cdot q + r \quad \text{with} \quad d(r) < d(b)$$
$$\text{or} \quad r = 0.$$

A Euclidean domain is an integral domain that admits a Euclidean function.

Theorem: Any Euclidean domain is a principal ideal domain.

Proof: Let R be a Euclidean domain with Euclidean function d. Let I be any ideal of R.

ideal of R.

If $I = \{0\}$ then $I = \langle 0 \rangle$ so I is principal

If $I \neq \{0\}$ then let $b \in I$ be

such that $d(b)$ is as small as possible.

If $a \in I$, there exist $q, r \in R$

such that $a = bq + r$ with $d(r) < d(b)$

or $r = 0$.

Then $r = \underbrace{\underbrace{a}_{\in I} - \underbrace{bq}_{\in I}}_{\in I}$. Since b was

an element of I with minimal value $d(b)$,

we must have $r = 0$. So in fact

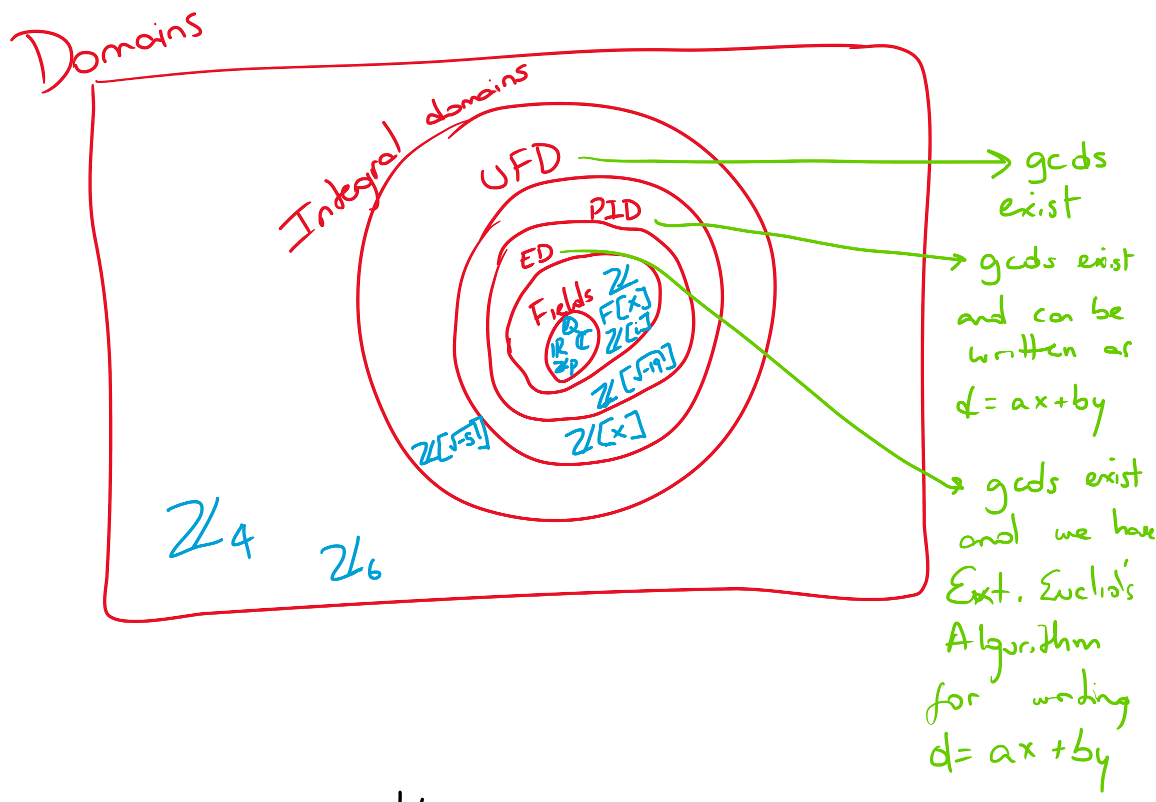
$$a = b \cdot q$$

showing that $I = \langle b \rangle$, so I is principal ∎

$R = \mathbb{R}[x]$ | $R = \mathbb{Z}[x]$ $I = \langle x, 2 \rangle$

R: Euclidean domain | $\mathbb{Z}[x]$: Not Euclidean domain; I: not principal

Picture



Fields:

A *field* is a domain (commutative ring with identity) in which every nonzero element is a unit (invertible).

Ex: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_p$ $\rightarrow$ prime.

Proposition: Suppose R is a domain. Then R is a field if and only if the only ideals of R are $\{0\}$ and R.

the only ideals of R are $\{0\}$ and R.

<u>Proof:</u> ($\Rightarrow$) Suppose R is a field. If I is an ideal of R that contains a nonzero element u, then, since u is a unit, I contains $\underset{\text{in } I}{u} \cdot \underset{\text{in } R}{u^{-1}} = \underset{\Rightarrow \text{ in } I}{1}$, and thus I contains $\underset{\text{in } I}{1} \cdot \underset{\text{in } R}{r} = \underset{\Rightarrow \text{ in } I}{r}$ for any $r \in R$, so $I = R$.

($\Leftarrow$) Suppose the only ideals of R are $\{0\}$ and R. Let $a \in R$ with $a \neq 0$.

Consider $\langle a \rangle$. Since $\langle a \rangle \supsetneq \{0\}$ then $\langle a \rangle = R$
($\langle a \rangle \supseteq \{0\}$ but $\langle a \rangle \neq \{0\}$)

This implies $1 \in \langle a \rangle$, so $1 = a \cdot b$ for some $b \in R$, showing that a is a unit. ∎

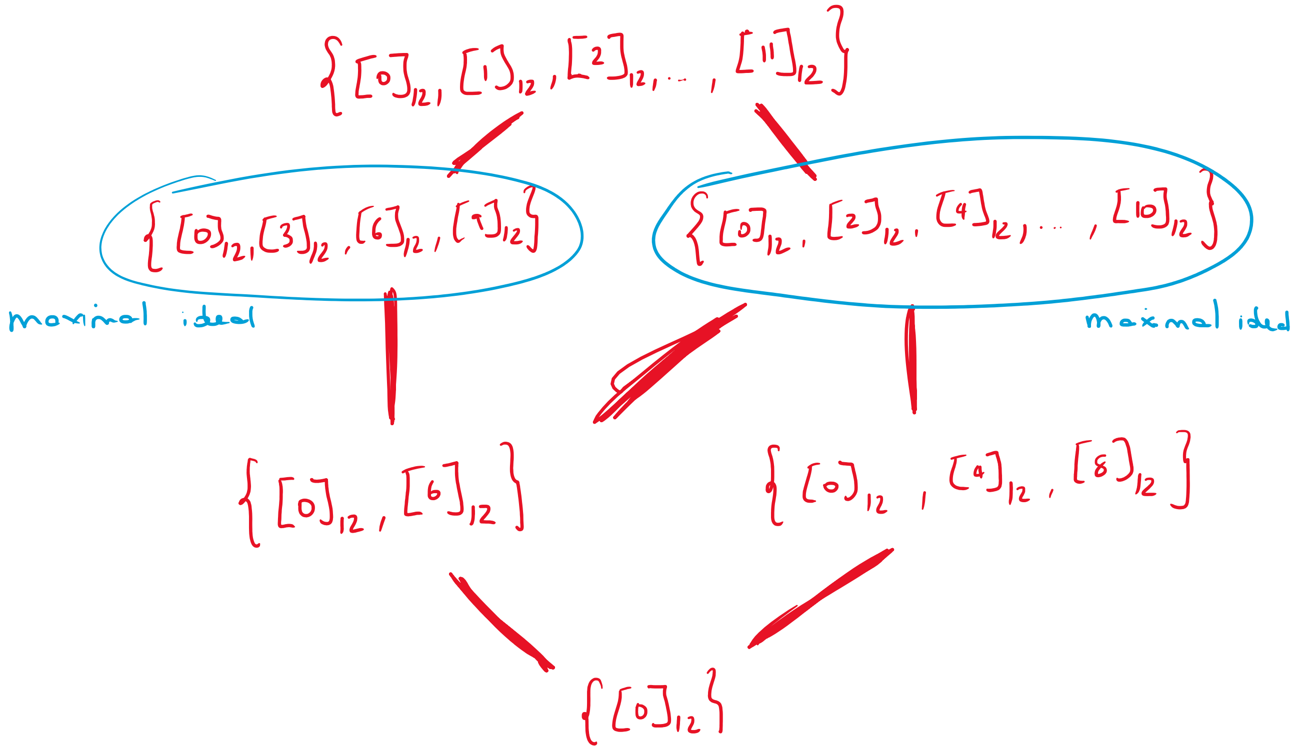
<u>Ex:</u> $\mathbb{Z}_{17}$. Take $[5]_{17}$. Consider $I = \langle [5]_{17} \rangle$

$\Rightarrow I = \mathbb{Z}_{17} \Rightarrow 1 = [5]_{17} \cdot b \Rightarrow [5]_{17}$ is a unit.

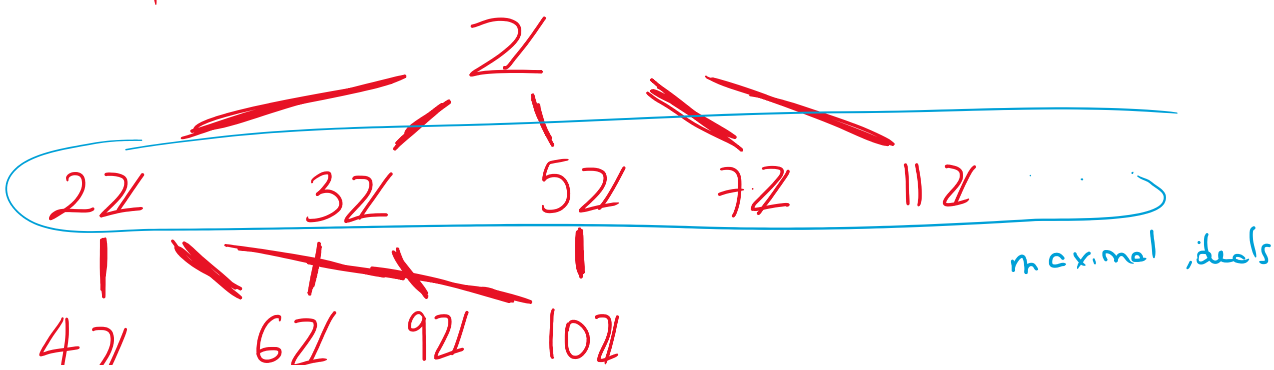
Definition: Let R be a domain.

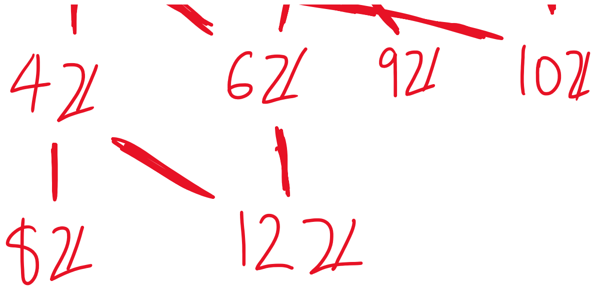
An ideal I of R is called a maximal ideal if $I \neq R$ there are no ideals containing I other than I and R.

Examples: Ideals of $\mathbb{Z}_{12}$:



Ideals of $\mathbb{Z}$:





Theorem: Let R be a domain, and I an ideal of R. Then

$$R/I \text{ is a field} \iff I \text{ is a maximal ideal.}$$

Proof: The Second Isomorphism Theorem says

$$\left\{ \begin{matrix} \text{ideals of} \\ R/I \end{matrix} \right\} \xleftrightarrow[\text{correspondence}]{\text{1-to-1}} \left\{ \begin{matrix} \text{ideals of } R \\ \text{that contain } I \end{matrix} \right\}$$

R/I is a field if and only if R/I has only two ideals (the zero ideal and R/I itself). This is the case precisely when there are only two ideals of R that contain I, which is equivalent to I being a maximal ideal. $\blacksquare$

Example: $R = \mathbb{R}[x]$

Is $\langle x^2-1 \rangle$ a maximal ideal?

$$x^2-1 = (x+1)(x-1)$$

No, $\langle x-1 \rangle \supsetneq \langle x^2-1 \rangle$.

Is $\langle x-1 \rangle$ a maximal ideal?

Yes: Any ideal in $\mathbb{R}[x]$ is principal, so if $\langle f \rangle \supseteq \langle x-1 \rangle$ then $f \mid x-1$, but since $x-1$ is irreducible,

$f = \text{unit} \cdot (x-1)$ (so $\langle f \rangle = \langle x-1 \rangle$)

or $f = \text{unit}$ (so $\langle f \rangle = \mathbb{R}[x]$).

Is $\langle x^3+2 \rangle$ a maximal ideal? $R = \mathbb{R}[x]$

$$x^3+2 = (x+\sqrt[3]{2}) \cdot (x^2 - \sqrt[3]{2}\,x + \sqrt[3]{4})$$

No: The ideal $\langle x+\sqrt[3]{2} \rangle \supsetneq \langle x^3+2 \rangle$.