Last time: PID $\Rightarrow$ UFD.

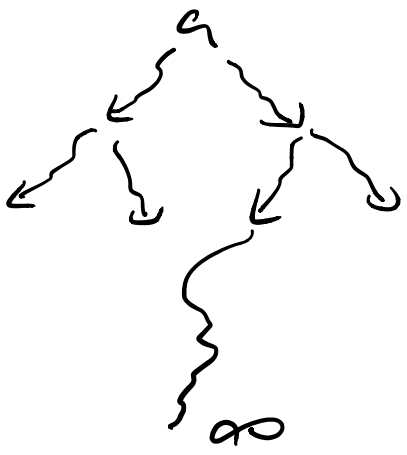
I tried to clean it up by defining the "length" of an element $a \in R$ as the length of the longest chain of ideals:

$$a_0R = aR \subsetneq a_1R \subsetneq \cdots \subsetneq a_\ell R = R.$$

But is it well-defined?

Yes, but the easiest way to prove this is to use the UFD property, so it's not really helpful for proving that PID $\Rightarrow$ UFD. //

So the proof that PIR $\Rightarrow$ every element factors into irreducibles looks like:



If factorization never terminates, we obtain an infinite chain of proper factors

$$aR \subsetneq a_1 R \subsetneq a_2 R \subsetneq \cdots$$

Contradiction.

Applications to $\mathbb{Z}$ & $\mathbb{F}[x]$:

$\mathbb{Z}$:

- units are ± 1, hence $a \sim b \iff a = \pm b$.
- every ideal is $n\mathbb{Z} \subseteq \mathbb{Z}$ for some unique $n \in \mathbb{N} = \{0, 1, 2, \ldots\}$.
- every prime ideal is $p\mathbb{Z} \subseteq \mathbb{Z}$ where p is usual prime or $p = 0$ (generic prime).
- every ring R has unique ring hom

$$\iota_R : \mathbb{Z} \to R,$$

where $\ker \iota_R = n\mathbb{Z} \subseteq \mathbb{Z}$. We define

the "characteristic of R" as

$$\mathrm{char}(R) = n \in \mathbb{N}.$$

- if R is a <u>domain</u> then

$$\mathbb{Z}/\ker \iota_R \cong \mathrm{im}\, \iota_R \subseteq R$$

is also a domain, hence $\ker \iota_R$ is a prime ideal, hence

$$\mathrm{char}(R) = 0 \quad \text{or}$$
$$\mathrm{char}(R) = p > 0,$$

- $\mathrm{char}(R) = 0$ means R contains $\mathbb{Z}$ as a subring. $\mathrm{char}(R) = p > 0$ means R contains $\mathbb{Z}/p\mathbb{Z}$ as subrings.

- if $R = \mathbb{F}$ is a field then

$\mathrm{char}(\mathbb{F}) = 0$ means $\mathbb{F} \supseteq \mathbb{Q} \supseteq \mathbb{Z}$, as subfield.

$\mathrm{char}(\mathbb{F}) = p > 0$ means $\mathbb{F} \supseteq \mathbb{Z}/p\mathbb{Z}$ as subfield.

In each case it is the <u>smallest</u> subfield, called the "prime subfield" of $\mathbb{F}$.

- If $\mathbb{F}$ is a finite field then $\text{char}(\mathbb{F}) = p > 0$. Since $\mathbb{F}$ is a finite dimensional vector space over $\mathbb{Z}/p\mathbb{Z}$, hence $\#\mathbb{F} = p^d$ where $d = \dim_{\mathbb{Z}/p\mathbb{Z}}(\mathbb{F})$.
- Conversely, $\exists$ unique field of size p^d for any prime $p > 0$ and power $d > 0$, but this is much harder to prove.

Applications to $\mathbb{F}[x]$:

- the units are nonzero constants, i.e., polynomials of degree zero.
- $f(x) \sim g(x) \iff f(x) = cg(x)$, $c \in \mathbb{F} \setminus 0$.
- every ideal is $m(x)\mathbb{F}[x] \subseteq \mathbb{F}[x]$

for some unique $m(x) \in \mathbb{F}[x]$ where

$m(x) = 0$

or

$m(x)$ has leading coeff $= 1$

"monic polynomial"

- prime ideals are $m(x)\mathbb{F}[x]$ where

$m(x) = 0$ (generic)

or

$m(x)$ is monic & irreducible ("prime")

- if $R \supseteq \mathbb{F}$ is a domain then for any $\alpha \in R$ we have the evaluation hom

$$\iota_\alpha : \mathbb{F}[x] \longrightarrow R$$
$$f(x) \longmapsto f(\alpha).$$

The image $\mathbb{F}[\alpha] \subseteq R$ is the smallest subring of R containing set $\mathbb{F} \cup \{\alpha\}$.

- Since R is a domain,

$$\mathbb{F}[x]/\ker \iota_\alpha \simeq \operatorname{im} \iota_\alpha = \mathbb{F}[\alpha] \subseteq R$$

domain

hence $\ker \iota_\alpha$ is prime:

$$\ker \iota_\alpha = m_\alpha(x)\, \mathbb{F}[x]$$

where $m_\alpha(x) = 0$

or

$m_\alpha(x)$ monic & irreducible.

- $m_\alpha(x) = 0 \iff \alpha$ transcendental $/\mathbb{F}$.

i.e. there is no nontrivial equation

$$f(\alpha) = 0.$$

Hence $\mathbb{F}[\alpha] \approx \mathbb{F}[x]/0 = \mathbb{F}[x]$.

Transcendental = "a variable"

- if $m_\alpha(x) \neq 0$ we say α is algebraic $/\mathbb{F}$ and we say

$m_\alpha(x) \in \mathbb{F}[x]$

is the "minimal polynomial" for $\alpha/\mathbb{F}$.

e.g. $m_{\sqrt{2}/\mathbb{Q}}(x) = x^2 - 2 \in \mathbb{Q}[x]$.

In this case, since nonzero prime ideal in PID is maximal, we conclude that

$$\mathbb{F}[x]/m_\alpha(x)\mathbb{F}(x) \approx \mathbb{F}[\alpha] \subseteq R$$

is actually a <u>field</u>. We write

$$\mathbb{F}[\alpha] = \mathbb{F}(\alpha) \subseteq R,$$

which is the smallest sub<u>field</u> of R containing the set $\mathbb{F} \cup \{\alpha\}$.

[Normally: $\mathbb{F}[\alpha] \subseteq \mathbb{F}(\alpha)$]

- Again, if $\alpha/\mathbb{F}$ is algebraic, so that $\mathbb{F}[x] = \mathbb{F}(\alpha)$ is a field, then $\mathbb{F}(\alpha)$ is a vector space $/\mathbb{F}$ with basis $1, \alpha, \alpha^2, \cdots, \alpha^{n-1}$ where

$$n = \deg(m_\alpha).$$

Proof: Spanning: Given any $f(\alpha) \in \mathbb{F}[\alpha]$

where $f(x) \in \mathbb{F}[x]$, divide to get

$$f(x) = q(x)\, m_\alpha(x) + r(x)$$

$$r(x) = 0 \quad \text{or} \quad \deg(r) < \deg(m_\alpha) = d.$$

Evaluate at α to get

$$f(\alpha) = q(\alpha)\underbrace{m_\alpha(\alpha)}_{0} + r(\alpha) = r(\alpha)$$

$$\| $$

$$r(\alpha) = c_0 + c_1\alpha + \cdots + c_{d-1}\alpha^{d-1} \quad \checkmark$$

Independence is the <u>uniqueness</u> of the remainder, i.e., suppose

$$r_1(\alpha) = r_2(\alpha) \qquad \deg(r_1), \deg(r_2) < d.$$

then $\underset{\deg < d}{r_1(x)} - \underset{\deg < d}{r_2(x)} \in \ker L_\alpha = m_\alpha(x)\,\mathbb{F}[x]$.

$$\Rightarrow \quad r_1(x) - r_2(x) = m_\alpha(x)\, q(x)$$

If $r_1(x) - r_2(x) \neq 0$, then this implies

$$\deg(m_\alpha) \leq \deg(r_1 - r_2) \quad \lightning$$