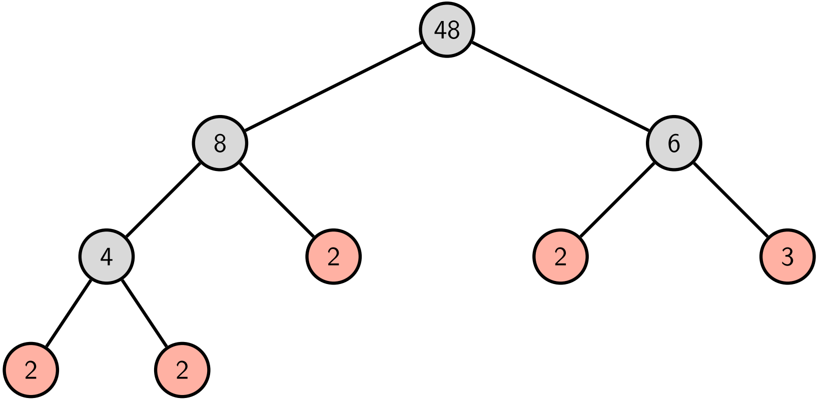
What is...a unique factorization domain?

Or: Primes!

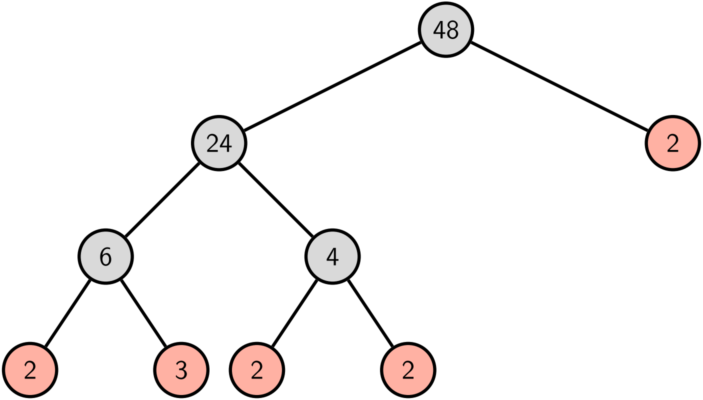
Factor trees – the leaves are the primes



Fundamental theorem of arithmetic – part 1. Factor trees exist

We want that for general rings, if possible

Factor trees are not unique, but...



Fundamental theorem of arithmetic – part 2. The leaves of factor trees are unique

We want that for general rings, if possible

What makes a prime a prime?

Definition 1. $p \in \mathbb{Z}$ is irreducible, that is

$$(p = ab) \Rightarrow (a \text{ is invertible or } b \text{ is invertible})$$

Definition 2. $p \in \mathbb{Z}$ is prime, that is

$$(p \text{ divides } ab) \Rightarrow (p \text{ divides } a \text{ or } b)$$

- In $\mathbb{Z}$ both definitions are equivalent
- Definition 1. Easy to prove existence of factorizations but uniqueness is hard
- Definition 2. Easy to prove uniqueness of factorizations but existence is hard

For completeness: The formal definition

An integral domain R is called a unique factorization domain (UFD) if

$$r \neq 0 \Rightarrow \exists \text{primes } p_k \text{ such that } r = sp_1^{e_1} \dots p_n^{e_n}$$

Here s is some invertible element

Thus, factor trees exist

(a) Such a factor tree always has unique leaves

(b) Alternatively, one could also demand that factor trees for irreducible elements exist and have unique leaves

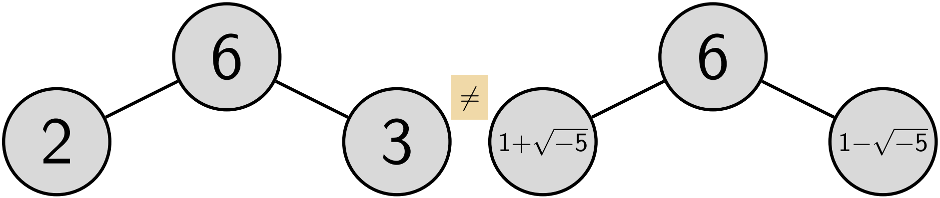
(c) In a UFD we have

$$\text{irreducible} \Leftrightarrow \text{prime}$$

Examples. Fields, $\mathbb{Z}$, $\mathbb{K}[X]$ for a field $\mathbb{K}$, $\mathbb{Z}[i]$, $\mathbb{Z}[e^{2\pi i/n}]$ for $n = 1, \dots, 22$, the ring of integers of $\mathbb{Q}[\sqrt{-d}]$ for $d = 1, 2, 3, 7, 11, 19, 43, 67, 163$

The standard non-example $\mathbb{Z}[\sqrt{-5}]$

- The invertible elements in $\mathbb{Z}[\sqrt{-5}]$ are ± 1
- 2 is irreducible
- 3 is irreducible
- $1 + \sqrt{-5}$ is irreducible
- $1 - \sqrt{-5}$ is irreducible
- None of these are primes!
- Unique factorization fails:



Thank you for your attention!

I hope that was of some help.