
# CSCI 740 - Programming Language Theory

Lecture 28

Gallois Connection

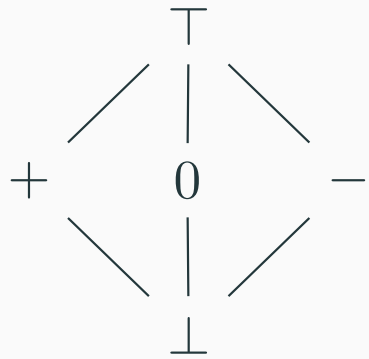
Instructor: Hossein Hojjat

November 8, 2017

# Abstract Domain

- An abstract domain is a lattice
- Elements in the lattice are called abstract values

**Example:** Sign Abstract Domain



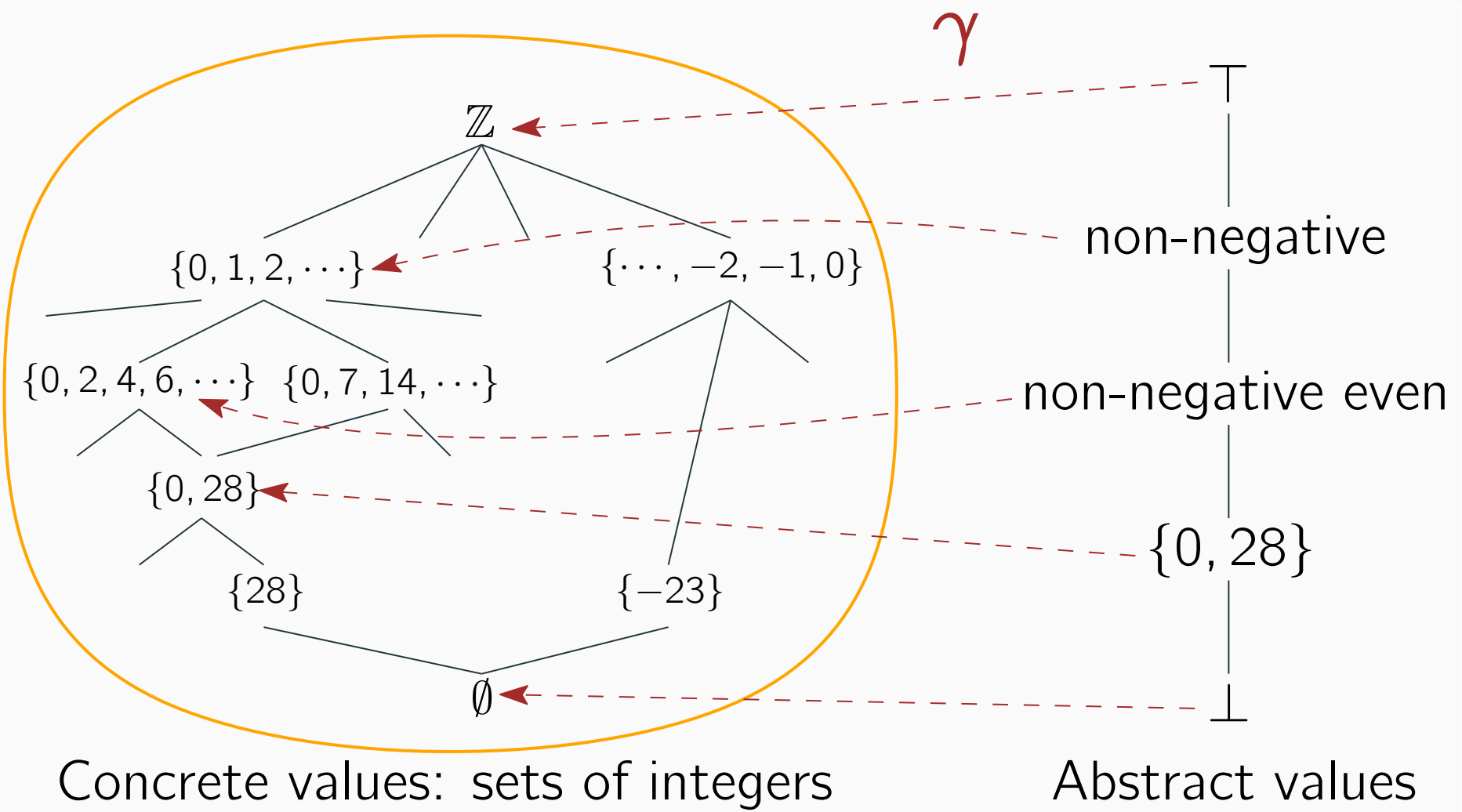

- Set of abstract values $\{\bot, +, 0, -, \top\}$
- Relation $\leq$ that is
  - Reflexive
  - Anti-symmetric
  - Transitive
- Least upper bound (lub, $\sqcup$) and greatest lower bound (glb, $\sqcap$) exists for any pair of elements
  - So it's a lattice

# $\alpha$ and $\gamma$

Need to relate elements in the lattice with concrete states in the program

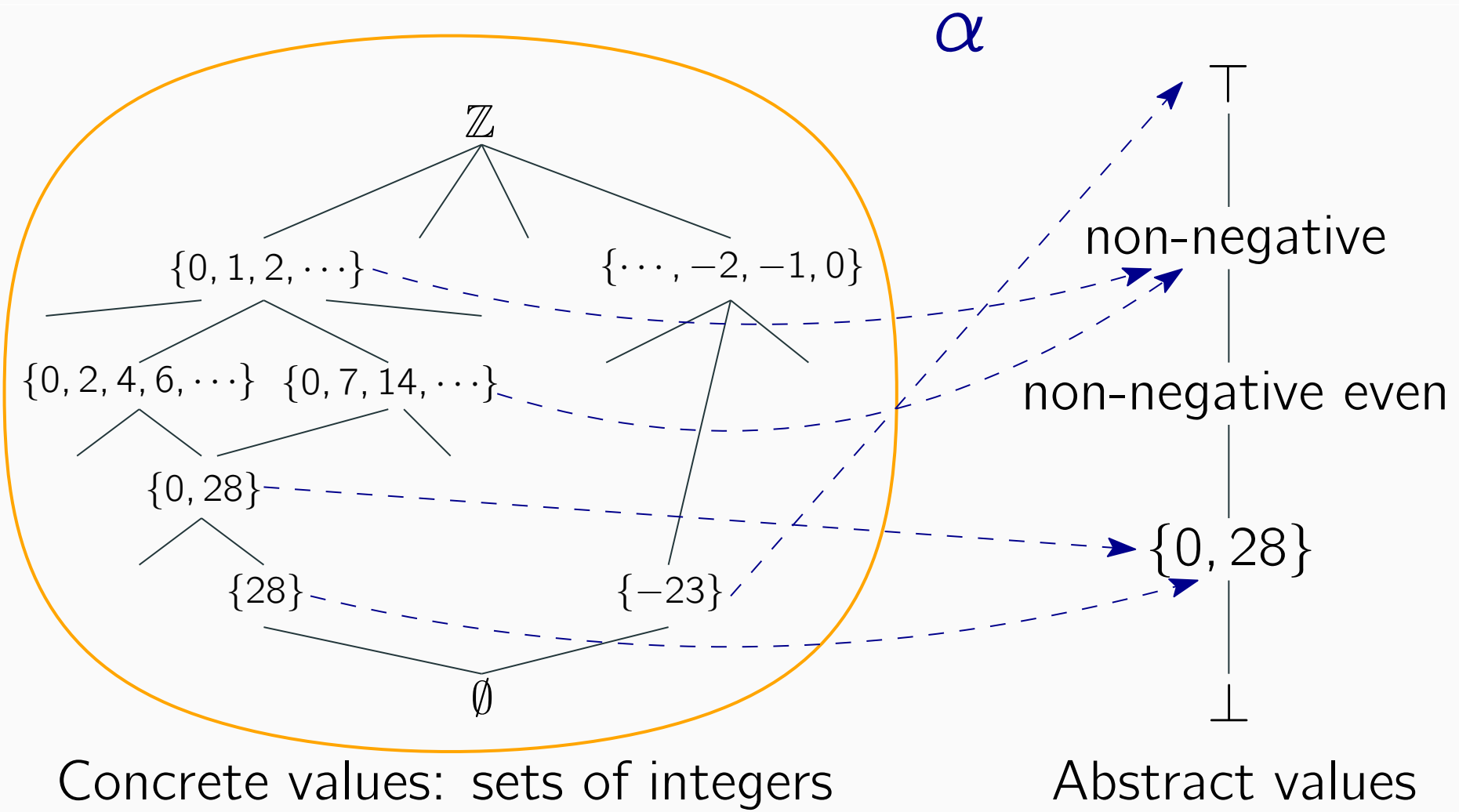
- **Abstraction Function:** $\alpha : 2^C \rightarrow \mathit{Abs}$
  Maps a value in the program to the "best" abstract value
- **Concretization Function:** $\gamma : \mathit{Abs} \rightarrow 2^C$
  Maps an abstract value to a set of values in the program

# Abstraction Example



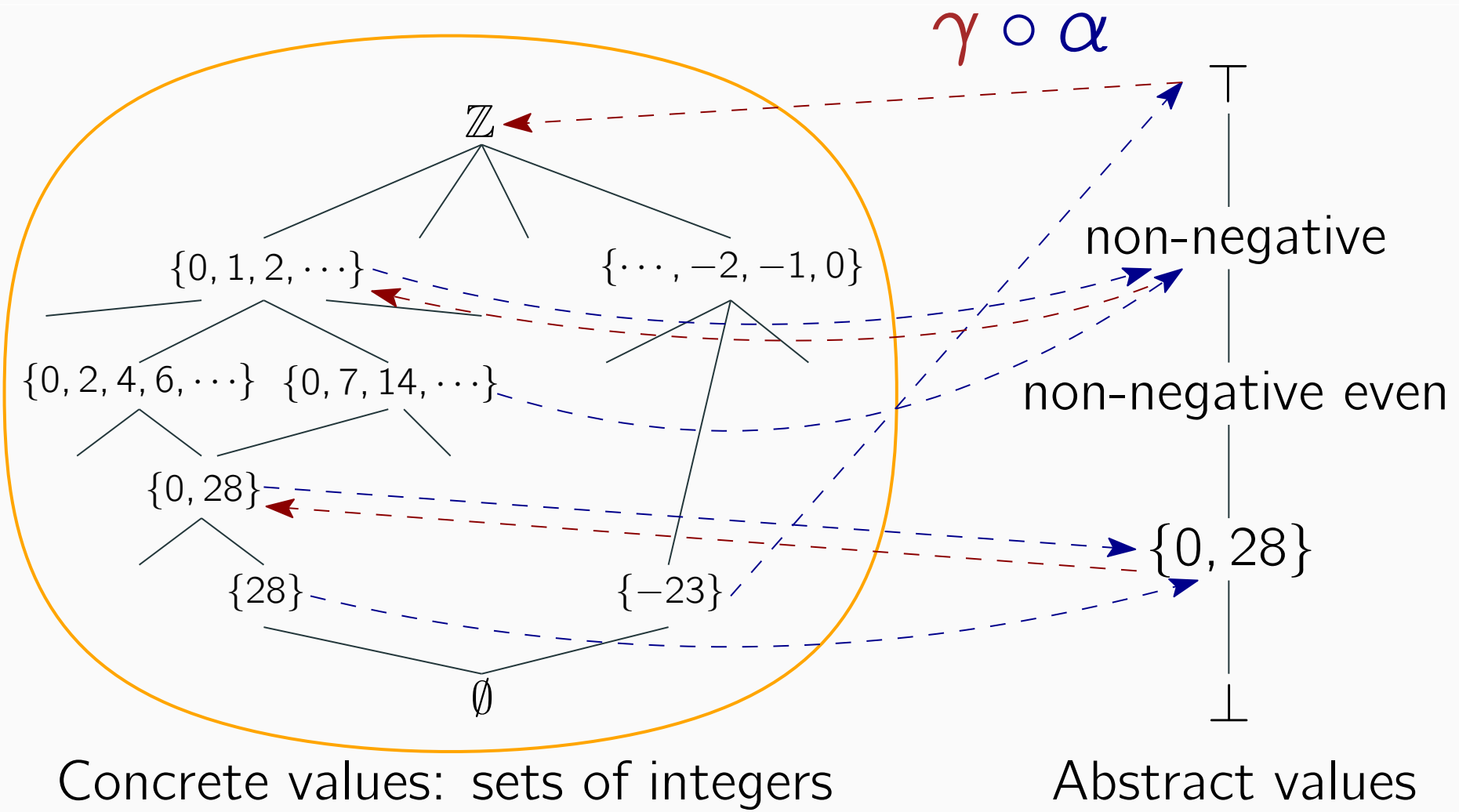

Concretization function $\gamma$ maps each abstract value to concrete values it represents

# Abstraction Example




Abstraction function $\alpha$ maps each concrete set to the best abstract value (least imprecise)

# Abstraction Example



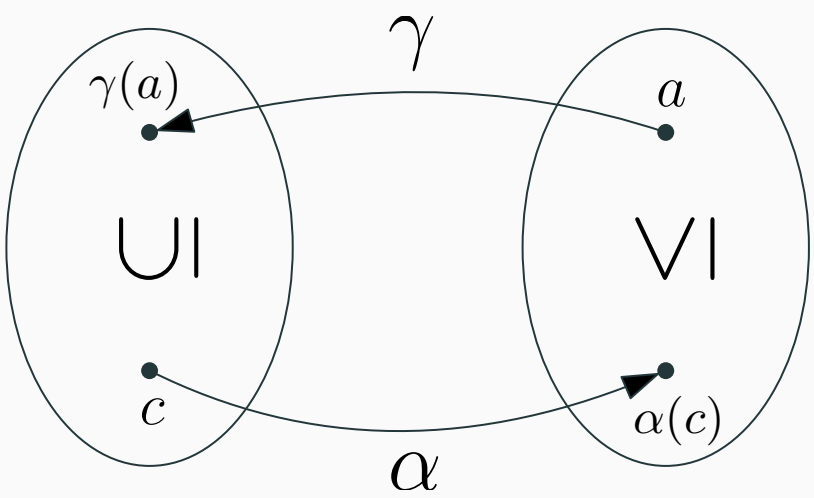

Abstraction followed by concretization is sound but imprecise

# Galois Connection

- $\alpha$ and $\gamma$ are monotonic
- Recall: $f$ is monotonic if $x \leq y \Rightarrow f(x) \leq f(y)$
- Also called "order preserving"

**Galois Connection:**

A pair of functions
(Abstraction) $\alpha : 2^C \rightarrow \mathit{Abs}$
and
(Concretization) $\gamma : \mathit{Abs} \rightarrow 2^C$
such that
$\forall a \in \mathit{Abs}. \forall c \in 2^C . c \subseteq \gamma(a) \Leftrightarrow \alpha(c) \leq a$



# Correctness Conditions

Three conditions guarantee correctness in general:

1. $\alpha$ and $\gamma$ are monotonic
2. $\alpha$ and $\gamma$ form a Galois connection
3. Abstract operations $\text{op}^A$ are locally correct

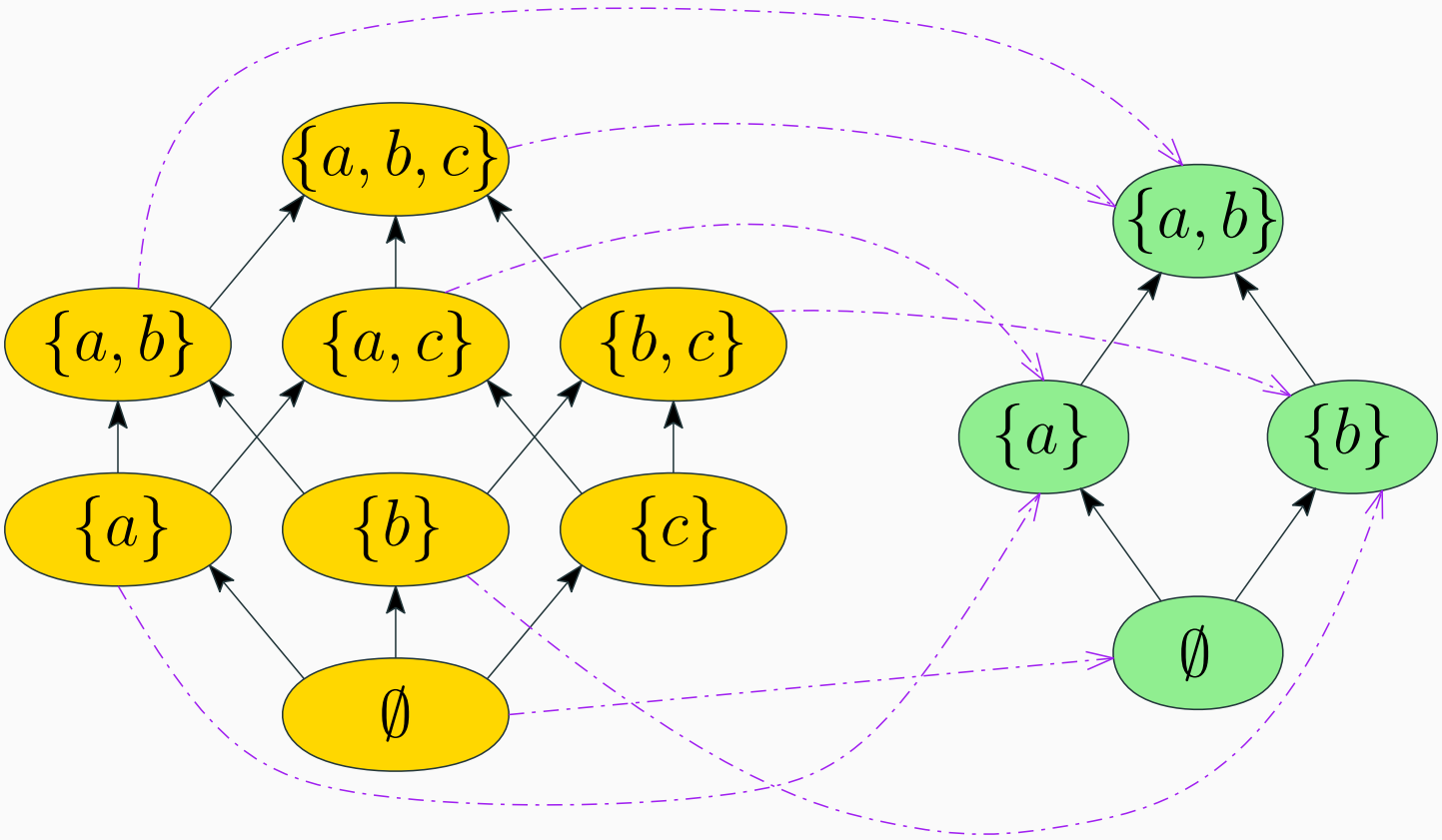
$$\gamma(a_1 \ \text{op}^A \ a_2) \supseteq \gamma(a_1) \ \text{op} \ \gamma(a_2)$$

# Key Property of Galois Connections

**Theorem.** The abstraction and concretization functions uniquely determine each other

$$\gamma(a) = \bigcup \{c \in 2^C \mid \alpha(c) \leq a\}$$
$$\alpha(c) = \bigsqcap \{a \in \mathit{Abs} \mid c \subseteq \gamma(a)\}$$

# Example




- $\gamma(\{a\}) = \cup\{\ell \mid \alpha(\ell) \leq \{a\}\} = \emptyset \cup \{a\} \cup \{a,c\} = \{a,c\}$
- $\gamma(\{b\}) = \cup\{\ell \mid \alpha(\ell) \leq \{b\}\} = \emptyset \cup \{b\} \cup \{b,c\} = \{b,c\}$
- $\gamma(\{a,b\}) = \emptyset \cup \{a,b\} \cup \{b,c\} \cup \cdots \cup \{a,b,c\} = \{a,b,c\}$