# Order Theory, Galois Connections and Abstract Interpretation

David Henriques

Carnegie Mellon University

November 7th 2011

# Order Theory

# Orders are everywhere

- $0 \leq 1$ and $1 \leq 10^{23}$
- Two cousins have a common grandfather
- $22/7$ is a worse approximation of $\pi$ than 3.141592654
- aardvark comes before zyzzyva
- a seraphim ranks above an angel
- rock beats scissors
- neither $\{1, 2, 4\}$ or $\{2, 3, 5\}$ are subsets of one another, but both are subsets of $\{1, 2, 3, 4, 5\}$

# Orders are everywhere

- $0 \leq 1$ and $1 \leq 10^{23}$
- Two cousins have a common grandfather
- $22/7$ is a worse approximation of $\pi$ than 3.141592654
- aardvark comes before zyzzyva
- a seraphim ranks above an angel
- rock beats scissors
- neither $\{1, 2, 4\}$ or $\{2, 3, 5\}$ are subsets of one another, but both are subsets of $\{1, 2, 3, 4, 5\}$

Actually, there is an intruder in this list. Can you spot it?

# Orders are everywhere

- $0 \leq 1$ and $1 \leq 10^{23}$
- Two cousins have a common grandfather
- $22/7$ is a worse approximation of $\pi$ than 3.141592654
- aardvark comes before zyzzyva
- a seraphim ranks above an angel
- rock beats scissors
- neither $\{1, 2, 4\}$ or $\{2, 3, 5\}$ are subsets of one another, but both are subsets of $\{1, 2, 3, 4, 5\}$

Actually, there is an intruder in this list. Can you spot it?
It's not easy, we need a formal treatment of order!

# What should we require from an order?

## Partial Order

Let $S$ be a set. A relation $\sqsubseteq$ in $S$ is said to be a **partial order relation** if it has the following properties

- if $a \sqsubseteq b$ and $b \sqsubseteq a$ then $b = a$ (anti-symmetry)
- if $a \sqsubseteq b$ and $b \sqsubseteq c$ then $a \sqsubseteq c$ (transitivity)
- $a \sqsubseteq a$ (reflexivity)

The pair $(S, \sqsubseteq)$ is said to be a **partial order**.

# What should we require from an order?

## Partial Order

Let $S$ be a set. A relation $\sqsubseteq$ in $S$ is said to be a **partial order relation** if it has the following properties

- if $a \sqsubseteq b$ and $b \sqsubseteq a$ then $b = a$ (anti-symmetry)
- if $a \sqsubseteq b$ and $b \sqsubseteq c$ then $a \sqsubseteq c$ (transitivity)
- $a \sqsubseteq a$ (reflexivity)

The pair $(S, \sqsubseteq)$ is said to be a **partial order**.

Why these properties?

# What should we require from an order?

## Partial Order

Let $S$ be a set. A relation $\sqsubseteq$ in $S$ is said to be a **partial order relation** if it has the following properties

- if $a \sqsubseteq b$ and $b \sqsubseteq a$ then $b = a$ (anti-symmetry)
- if $a \sqsubseteq b$ and $b \sqsubseteq c$ then $a \sqsubseteq c$ (transitivity)
- $a \sqsubseteq a$ (reflexivity)

The pair $(S, \sqsubseteq)$ is said to be a **partial order**.

Why these properties?

- they correspond to intuitive notions of order
- structures that share these properties have a lot of common behavior

# Examples - Natural Numbers

$$(\mathbb{N}, \leq)$$

# Examples - Natural Numbers

$$(\mathbb{N}, \leq)$$

- if $a \leq b$ and $b \leq a$ then $a = b$

# Examples - Natural Numbers

$$(\mathbb{N}, \leq)$$

- if $a \leq b$ and $b \leq a$ then $a = b$
- if $a \leq b$ and $b \leq c$ then $a \leq c$

# Examples - Natural Numbers

$$(\mathbb{N}, \leq)$$

- if $a \leq b$ and $b \leq a$ then $a = b$
- if $a \leq b$ and $b \leq c$ then $a \leq c$
- $a \leq a$

# Examples - Natural Numbers

$$(\mathbb{N}, \leq)$$

- if $a \leq b$ and $b \leq a$ then $a = b$
- if $a \leq b$ and $b \leq c$ then $a \leq c$
- $a \leq a$

Well... this was not very informative

# Examples - Rock, paper, scissors

({}, "beats")

# Examples - Rock, paper, scissors

({✄, 🗏, ◯}, "beats")

- We don't have that ✄ beats ✄

# Examples - Rock, paper, scissors

Let's try again

({, , }, "is not beaten by")

# Examples - Rock, paper, scissors

Let's try again
({✂, 🗎, 🪨}, "is not beaten by")

- It's reflexive (e.g. ✂ is not beaten by ✂)

# Examples - Rock, paper, scissors

Let's try again

({✂, 📄, 🪨}, "is not beaten by")

- It's reflexive (e.g. ✂ is not beaten by ✂)
- It's antisymmetric (e.g. ✂ is not beaten by 📄 means we can't heave 📄 is not beaten by ✂)

# Examples - Rock, paper, scissors

Let's try again

({✂, 📄, 🪨}, "is not beaten by")

- It's reflexive (e.g. ✂ is not beaten by ✂)
- It's antisymmetric (e.g. ✂ is not beaten by 📄 means we can't heave 📄 is not beaten by ✂)
- It's NOT transitive (✂ is not beaten by 📄 is not beaten by 🪨. But We don't have that ✂ is not beaten by 🪨)

# Examples - Subset inclusion

$$(\mathcal{P}(S), \subseteq)$$

# Examples - Subset inclusion

$$(\mathcal{P}(S), \subseteq)$$

- if $P \subseteq Q$ and $P \subseteq Q$ then $P = Q$

# Examples - Subset inclusion

$$(\mathcal{P}(S), \subseteq)$$

- if $P \subseteq Q$ and $P \subseteq Q$ then $P = Q$
- if $P \subseteq Q$ and $Q \subseteq R$ then $P \subseteq R$

# Examples - Subset inclusion

$$(\mathcal{P}(S), \subseteq)$$

- if $P \subseteq Q$ and $P \subseteq Q$ then $P = Q$
- if $P \subseteq Q$ and $Q \subseteq R$ then $P \subseteq R$
- $P \subseteq P$

# Examples - Subset inclusion

What about sets like $\{1, 2, 4\}$ and $\{3, 4, 5\}$, which one is “bigger”?

# Examples - Subset inclusion

What about sets like $\{1, 2, 4\}$ and $\{3, 4, 5\}$, which one is “bigger”?

Well... none

In general, we don’t require all elements to be comparable amongst themselves.

# Examples - Subset inclusion

What about sets like $\{1, 2, 4\}$ and $\{3, 4, 5\}$, which one is "bigger"?

Well... none

In general, we don't require all elements to be comparable amongst themselves.

## Total Order

Let $(S, \sqsubseteq)$ be a partial order. Then $(S, \sqsubseteq)$ is called a **total order** if

- for all $a, b \in S$, $a \sqsubseteq b$ or $b \sqsubseteq a$ (totality)

# Examples - Subset inclusion induced orders

Subset inclusion induces orderings in may algebraic structures

# Examples - Subset inclusion induced orders

Subset inclusion induces orderings in may algebraic structures

- subgroup orderings (used in Galois Theory)
- subfield orderings (aka towers, also used in GT)
- subspaces (used in linear Algebra and Geometry)
- ideals of rings (used pretty much everywhere)
- ...

# Bounds, suprema, infima

Let $(S, \sqsubseteq)$ be a partial order and $P \subseteq S$. An element $b \in S$ is said to be:

- an **upper bound** of $P$ if $\forall p \in P, b \sqsubseteq b$
- a **lower bound** of $P$ if $\forall p \in P, b \sqsubseteq p$
- the **supremum** of $P$ if b is the least upper bound of $P$:
  $b$ is u.b. of $P$ and if $b'$ is an u.b. of $P$, $b \sqsubseteq b'$
- the **infimum** of $P$ if b is the greatest lower bound of $P$:
  $b$ is l.b. of $P$ and if $b'$ is a l.b. of $P$, $b' \sqsubseteq b$

# Meet and Join

The functions that return suprema and infima are called, respectively, **join** and **meet**:

### meet and join

- $\bigwedge : \mathcal{P}(S) \rightarrow S$, $\bigwedge(P) = b$, $b$ infimum of $P$ is the meet function.
- $\bigvee : \mathcal{P}(S) \rightarrow S$, $\bigvee(P) = b$, $b$ supremum of $P$ is the join function.

# Warning

Suprema and infima are not guaranteed to exist!

# Warning

Suprema and infima are not guaranteed to exist!

Fortunately, we will generally work in structures where meets and joins exist!

# Lattices

## Lattice

Let $(S, \sqsubseteq)$ be a partial order. $(S, \sqsubseteq)$ is a **lattice** if the meet and join of any pair of elements of $S$ always exists.

# Lattices

## Lattice

Let $(S, \sqsubseteq)$ be a partial order. $(S, \sqsubseteq)$ is a **lattice** if the meet and join of any pair of elements of $S$ always exists.

## Complte Lattice

Let $(S, \sqsubseteq)$ be a partial order. $(S, \sqsubseteq)$ is a **complete lattice** if the meet and join of any subset of elements of $S$ always exists.

# Lattices

## Lattice

Let $(S, \sqsubseteq)$ be a partial order. $(S, \sqsubseteq)$ is a **lattice** if the meet and join of any pair of elements of $S$ always exists.

## Complte Lattice

Let $(S, \sqsubseteq)$ be a partial order. $(S, \sqsubseteq)$ is a **complete lattice** if the meet and join of any subset of elements of $S$ always exists.

## Top and Bottom

Let $(S, \sqsubseteq)$ be a complete Lattice. Then

- $\top = \bigvee S$ is an u. b. of any subset of $S$ and called the **top** of S
- $\bot = \bigwedge S$ is a l. b. of any subset of $S$ and called the **bottom** of S

# Monotonicity and Continuity

## Monotonicity and Continuity

Let $(S, \sqsubseteq)$ be a complete lattice. Let $f : S \to S$ be a function. We say $f$ is

- **monotonic** if, for $a \sqsubseteq b$, then $f(a) \sqsubseteq f(b)$
- $\bigvee$-**continuous** if, for every $a_1 \sqsubseteq a_2 \sqsubseteq \ldots$, then $f(\bigvee a_i) = \bigvee f(a_i)$
- $\bigwedge$-**continuous** if, for every $a_1 \sqsupseteq a_2 \sqsupseteq \ldots$, then $f(\bigwedge a_i) = \bigwedge f(a_i)$

# An old f(r)iend revisited

## Tarski's fixed point lemma

Let $(S, \sqsubseteq)$ be a complete lattice. Let $f : S \to S$ be a monotonic function.
Then the set of fixed points of $f$ is also a complete lattice.
In particular it has a top (the **gfp** of f) and a bottom (the **lfp** of f)

# Galois Connections

# Monotone Galois Connection

Let $\langle X, \leq \rangle$ and $\langle Y, \sqsubseteq \rangle$ be complete lattices. Let $L : X \to Y$ and $U : Y \to X$.

Then we say that $(\langle X, \leq \rangle, \langle Y, \sqsubseteq \rangle), L, U$ is a (monotone) Galois Connection if, for all $x \in X, y \in Y$:

$$L(x) \sqsubseteq y \text{ iff } x \leq U(y)$$

$L$ is called the lower adjoint (of $U$) and $U$ is called the upper adjoint (of $L$).

# Examples

- $L(x) = \bot_Y$

# Examples

- $L(x) = \bot_Y$ , $U(y) = \top_X$

# Examples

- $L(x) = \bot_Y$ , $U(y) = \top_X$
- $X = 2\mathbb{N}, Y = 2\mathbb{N} + 1, L(x) = x + 1$

# Examples

- $L(x) = \bot_Y \ , U(y) = \top_X$
- $X = 2\mathbb{N}, Y = 2\mathbb{N} + 1, L(x) = x + 1, U(y) = y - 1$

# Examples

- $L(x) = \bot_Y$ , $U(y) = \top_X$
- $X = 2\mathbb{N}, Y = 2\mathbb{N} + 1, L(x) = x + 1, U(y) = y - 1$
- $X = 2\mathbb{N}, Y = 2\mathbb{N} + 1, L(x) = x + 3$

# Examples

- $L(x) = \bot_Y$ , $U(y) = \top_X$
- $X = 2\mathbb{N}, Y = 2\mathbb{N} + 1, L(x) = x + 1, U(y) = y - 1$
- $X = 2\mathbb{N}, Y = 2\mathbb{N} + 1, L(x) = x + 3, U(y) = y - 3$

# Examples

- $L(x) = \bot_Y$ , $U(y) = \top_X$
- $X = 2\mathbb{N}, Y = 2\mathbb{N} + 1, L(x) = x + 1, U(y) = y - 1$
- $X = 2\mathbb{N}, Y = 2\mathbb{N} + 1, L(x) = x + 3, U(y) = y - 3$
- $X, Y, L$ is a bijective function, $U = L^{-1}$

# Examples - The Functional Abstraction

Let $S_1$ and $S_2$ be sets, $f : S_1 \to S_2$ and

$$L(A) = \{f(a)|a \in A\} \qquad U(B) = \{a|f(a) \in B\}$$

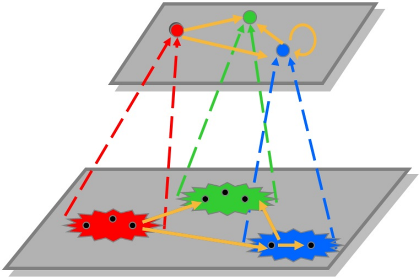
Then

$$(\langle \mathcal{P}(S_1), \subseteq \rangle, \langle \mathcal{P}(S_2), \subseteq \rangle, L, U)$$

is a Galois Connection.

Proof: $L(A) = \{f(a)|a \in A\} \subseteq B$ iff $\forall_{a \in A} f(a) \in B$ iff
$A \subseteq \{a|f(a) \in B\} = U(B)$

# Why is this useful?



# Duality

Let $\langle X, \leq\rangle, \langle Y, \sqsubseteq\rangle, L, U$ be a Galois connection,
Then $\langle Y, \sqsupseteq\rangle, \langle X, \geq\rangle, U, L$ is a Galois connection.

Proof: $L(x) \sqsubseteq y$ iff $x \leq U(y) \quad \Leftrightarrow \quad U(y) \geq x$ iff $y \sqsupseteq L(x)$

# Composition

Let $\langle X, \leq \rangle, \langle Y, \sqsubseteq \rangle, L_1, U_1$ and $\langle Y, \sqsubseteq \rangle, \langle Z, \preceq \rangle, L_2, U_2$ be GCs.
Then $\langle X, \leq \rangle, \langle Z, \preceq \rangle, L_2 \circ L_1, U_1 \circ U_2$ is a GC

Proof:
$L_2(y) \preceq z$ iff $y \sqsubseteq U_2(z)$. Take $y = L_1(x)$.
Then $L_2(L_1(x)) \preceq z$ iff $L_1(x) \sqsubseteq U_2(z)$ iff $x \leq U_1(U_2(z))$

# Cancellation and Monotonicity

Let $\langle X, \leq \rangle, \langle Y, \sqsubseteq \rangle, L, U$ be GC.
Then

1. $x \leq U(L(x))$ and $L(U(y)) \sqsubseteq y$
2. Both $U$ and $L$ are monotonic.

Proof:

1. $L(x) \sqsubseteq L(x)$ iff $x \leq U(L(x))$
2. $x \leq x' \Rightarrow_1 x \leq U(L(x'))$
   $x \leq U(L(x'))$ iff $L(x) \sqsubseteq L(x')$

# Preservation of Infima and Suprema

Let $\langle X, \leq \rangle, \langle Y, \sqsubseteq \rangle, L, U$ be a GC.
Then $L$ preserves suprema and $U$ preserves infima, i.e.

$$L(\bigvee X') = \bigsqcup L(X') \text{ and } U(\bigwedge Y') = \bigsqcap U(Y')$$

Proof:
Let $X' \ni x \leq \bigvee X'$. By monotonicity of $L$, $L(x) \sqsubseteq L(\bigvee X')$ and $L(\bigvee X')$ is therefore an upper bound of $L(X')$.
Let $y$ be another UB of $L(X')$. Then, for all $x \in X'$, $L(x) \sqsubseteq y$ iff, by def, $x \leq U(y)$. But then $\bigvee X' \leq U(y)$ iff, by def, $L(\bigvee X') \sqsubseteq y$, therefore $L(\bigvee X')$ is the lowest upper bound of $L(X')$.

# Existence

Let $\langle X, \leq \rangle, \langle Y, \sqsubseteq \rangle$ and $L : X \to Y$ such that $L$ preserves suprema.
Then there exists $U$ s.t. $\langle X, \leq \rangle, \langle Y, \sqsubseteq \rangle, L, U$ is a GC.

Proof:
Let $U = \lambda y. \bigvee \{x : L(x) \sqsubseteq y\}$.

$$L(x) \sqsubseteq y \Rightarrow x \in \{z : L(z) \sqsubseteq y\} \Rightarrow x \leq \bigvee \{z : L(z) \sqsubseteq y\}$$
$$\Leftrightarrow x \leq U(y).$$

$$x \leq U(y) \Rightarrow L(x) \sqsubseteq L(\bigvee \{z : L(z) \sqsubseteq y\}) \qquad L \text{ monotonic}$$
$$\Rightarrow L(x) \sqsubseteq \bigsqcup \{L(z) : L(z) \sqsubseteq y\} \qquad L \text{ preserves suprema}$$
$$\Rightarrow L(x) \sqsubseteq y$$

# Transfer Theorem

Let $\langle X, \leq \rangle$,$\langle Y, \sqsubseteq \rangle$ $F : X \rightarrow X$ monotonic, $F' : Y \rightarrow Y$ monotonic and $L : X \rightarrow Y$ preserving suprema.

Then

$$L \circ F \sqsubseteq F' \circ L \quad \text{iff} \quad L(\text{lfp}[F]) \sqsubseteq \text{lfp}[F']$$

# Fixpoint Approximation Theorem

Let $\langle X, \leq \rangle$,$\langle Y, \sqsubseteq \rangle$ $F : X \to X$ monotonic and $L : X \to Y$ preserving suprema.

Then, there is $F' : Y \to Y$ monotonic s.t.

$$\text{lfp}[F] \leq U(\text{lfp}[F'])$$

where $U$ is the upper adjoint of $L$.

"Proof": Take $F' = L \circ F \circ U$. Apply the Transfer Theorem to get

$$L(\text{lfp}[F]) \sqsubseteq \text{lfp}[F']$$

Now apply $U$, which is continuous to both sides and get the result by Cancellation on the left.

# References

M. Erné, J. Koslowski, A. Melton and G.E. Strecker
A primer on Galois Connections,
*York Academy of Science*, 1992.

P. Cousot and R. Cousot
Galois Connection based abstract interpretations for strictness analysis,
*International Conference on Formal Methods in Programming and their Applications*, 1993.

R. Backhouse
Galois Connections and Fixed Point Calculus,
*Algebraic and Coalgebraic Methods in the Mathematics of Program Construction*, 2002.

Time permitting

How everything you've ever seen was thought of by Galois!

# Examples

$$n \leq \lfloor x \rfloor \text{ iff } n \leq x$$

# Examples

$$n \leq \lfloor x \rfloor \text{ iff } n \leq x$$

$$\text{real}(n) \leq x \text{ iff } n \leq \text{floor}(x)$$

# Examples

$$n \leq \lfloor x \rfloor \text{ iff } n \leq x$$

$$\text{real}(n) \leq x \text{ iff } n \leq \text{floor}(x)$$

$\lfloor x \rfloor \leq x$

# Examples

$$n \leq \lfloor x \rfloor \text{ iff } n \leq x$$

$$\text{real}(n) \leq x \text{ iff } n \leq \text{floor}(x)$$

$\lfloor x \rfloor \leq x$

$\quad \lfloor x \rfloor \leq \lfloor x \rfloor \text{ iff } \lfloor x \rfloor \leq x$

# Examples

$$n \leq \lfloor x \rfloor \text{ iff } n \leq x$$

$$\text{real}(n) \leq x \text{ iff } n \leq \text{floor}(x)$$

$\lfloor x \rfloor \leq x$

$$\lfloor x \rfloor \leq \lfloor x \rfloor \text{ iff } \lfloor x \rfloor \leq x$$

$n \leq \lfloor n \rfloor$

# Examples

$$n \leq \lfloor x \rfloor \text{ iff } n \leq x$$

$$\text{real}(n) \leq x \text{ iff } n \leq \text{floor}(x)$$

$\lfloor x \rfloor \leq x$

$$\lfloor x \rfloor \leq \lfloor x \rfloor \text{ iff } \lfloor x \rfloor \leq x$$

$n \leq \lfloor n \rfloor$

$$n \leq \lfloor n \rfloor \text{ iff } n \leq n$$

# Examples

$$n \leq \lfloor x \rfloor \text{ iff } n \leq x$$

$$\text{real}(n) \leq x \text{ iff } n \leq \text{floor}(x)$$

$\lfloor x \rfloor \leq x$

$$\lfloor x \rfloor \leq \lfloor x \rfloor \text{ iff } \lfloor x \rfloor \leq x$$

$n \leq \lfloor n \rfloor \wedge \lfloor n \rfloor \leq n \quad \Leftrightarrow \quad n = \lfloor n \rfloor$

$$n \leq \lfloor n \rfloor \text{ iff } n \leq n$$

# Examples

$$n \leq \lfloor x \rfloor \text{ iff } n \leq x$$

$$\text{real}(n) \leq x \text{ iff } n \leq \text{floor}(x)$$

$\lfloor x \rfloor \leq x$

$\qquad \lfloor x \rfloor \leq \lfloor x \rfloor \text{ iff } \lfloor x \rfloor \leq x$

$n \leq \lfloor n \rfloor \wedge \lfloor n \rfloor \leq n \quad \Leftrightarrow \quad n = \lfloor n \rfloor$

$\qquad n \leq \lfloor n \rfloor \text{ iff } n \leq n$

$x \leq y \Rightarrow \lfloor x \rfloor \leq \lfloor y \rfloor$

# Examples

$$n \leq \lfloor x \rfloor \text{ iff } n \leq x$$

$$\text{real}(n) \leq x \text{ iff } n \leq \text{floor}(x)$$

$\lfloor x \rfloor \leq x$

$\quad \lfloor x \rfloor \leq \lfloor x \rfloor \text{ iff } \lfloor x \rfloor \leq x$

$n \leq \lfloor n \rfloor \wedge \lfloor n \rfloor \leq n \quad \Leftrightarrow \quad n = \lfloor n \rfloor$

$\quad n \leq \lfloor n \rfloor \text{ iff } n \leq n$

$x \leq y \Rightarrow \lfloor x \rfloor \leq \lfloor y \rfloor$

$\quad x \leq y \Rightarrow \lfloor x \rfloor \leq x \leq y \Rightarrow \lfloor x \rfloor \leq y$

# Examples

$$n \leq \lfloor x \rfloor \text{ iff } n \leq x$$

$$\mathrm{real}(n) \leq x \text{ iff } n \leq \mathrm{floor}(x)$$

$\lfloor x \rfloor \leq x$

$\quad \lfloor x \rfloor \leq \lfloor x \rfloor \text{ iff } \lfloor x \rfloor \leq x$

$n \leq \lfloor n \rfloor \wedge \lfloor n \rfloor \leq n \quad \Leftrightarrow \quad n = \lfloor n \rfloor$

$\quad n \leq \lfloor n \rfloor \text{ iff } n \leq n$

$x \leq y \Rightarrow \lfloor x \rfloor \leq \lfloor y \rfloor$

$\quad x \leq y \Rightarrow \lfloor x \rfloor \leq x \leq y \Rightarrow \lfloor x \rfloor \leq y$

$\quad \lfloor x \rfloor \leq y \text{ iff } \lfloor x \rfloor \leq \lfloor y \rfloor$

# Examples

- $p \wedge q \Rightarrow r$ iff $q \Rightarrow p \Rightarrow r$

# Examples

- $p \wedge q \Rightarrow r$ iff $q \Rightarrow p \Rightarrow r$
  $X, Y = P, \langle X, \Rightarrow \rangle, \langle Y, \Rightarrow \rangle$, $L = (p \wedge .), U = (p \Rightarrow .)$

# Examples

- $p \wedge q \Rightarrow r$ iff $q \Rightarrow p \Rightarrow r$
  $X, Y = P, \langle X, \Rightarrow \rangle, \langle Y, \Rightarrow \rangle,\ L = (p \wedge .), U = (p \Rightarrow .)$
- $\neg p \Rightarrow q$ iff $p \Leftarrow \neg q$

# Examples

- $p \wedge q \Rightarrow r$ iff $q \Rightarrow p \Rightarrow r$
  $X, Y = P, \langle X, \Rightarrow \rangle, \langle Y, \Rightarrow \rangle,\ L = (p \wedge .), U = (p \Rightarrow .)$
- $\neg p \Rightarrow q$ iff $p \Leftarrow \neg q$
  $X, Y = P, \langle X, \Leftarrow \rangle, \langle Y, \Rightarrow \rangle,\ L, U = \neg(.)$

# Examples

- $p \wedge q \Rightarrow r$ iff $q \Rightarrow p \Rightarrow r$
  $X, Y = P, \langle X, \Rightarrow \rangle, \langle Y, \Rightarrow \rangle,\ L = (p \wedge .), U = (p \Rightarrow .)$
- $\neg p \Rightarrow q$ iff $p \Leftarrow \neg q$
  $X, Y = P, \langle X, \Leftarrow \rangle, \langle Y, \Rightarrow \rangle,\ L, U = \neg(.)$
- Given $R \subseteq A \times B$
  $\langle \mathcal{P}(A), \subseteq \rangle, \langle \mathcal{P}(B), \subseteq \rangle,$
  $L(M) = \{b : aRb, a \in M\}, U(M) = \{a : aRb, b \in M\}$
  (antitone GC)

# Examples

- Given field $K$
  $\langle K[x_1, ...x_n], \subseteq\rangle$, $\langle K^n, \subseteq\rangle$,
  $L(I) = \{x \in K^n : \forall f \in I.f(x) = 0\}$,
  $U(V) = \{f \in K[x_1, ...x_n] : \forall x \in V.f(x) = 0\}$

# Examples

- Given field $K$
  $\langle K[x_1, ...x_n], \subseteq\rangle$, $\langle K^n, \subseteq\rangle$,
  $L(I) = \{x \in K^n : \forall f \in I.f(x) = 0\}$,
  $U(V) = \{f \in K[x_1, ...x_n] : \forall x \in V.f(x) = 0\}$
- Given mathematical structure $M$ over set $X$
  $L(S) =$ substructure generated by $S$ ($S \subseteq X$)
  $U(N) =$ underlying set of substructure $N$

Even more time permitting

Fixed points, closures and isomorphisms

# Order Isomorphisms

An order isomorphism between $\langle X, \leq \rangle$,$\langle Y, \sqsubseteq \rangle$ is a surjective function $h : X \rightarrow Y$ that is an order embedding, that is,

$$h(x) \sqsubseteq h(x') \text{ iff } x \leq x'$$

Order isomorphic posets can be considered to be "essentially the same" in the sense that one of them can be obtained from the other just by renaming of elements.

# Some Lemmas

Let $\langle X, \leq \rangle, \langle Y, \sqsubseteq \rangle, L, U$ be a GC.

Then

$$L(U(L(x))) = L(x) \text{ and } U(L(U(y))) = U(y)$$

Proof:
($\sqsubseteq$) By Cancellation, $x \leq U(L(x))$. By monotonicity of $L$, $L(x) \sqsubseteq L(U(L(x)))$.
($\sqsupseteq$) $L(U(L(x))) \sqsubseteq L(x)$ iff $U(L(x)) \leq U(L(x))$ by definition of GC.

# Some Lemmas

Let $\langle X, \leq \rangle, \langle Y, \sqsubseteq \rangle, L, U$ be a GC.

Then
$x \in U(Y)$ iff $x$ is a fixed point of $U \circ L$ and $y \in L(X)$ iff $y$ is a fixed point of $L \circ U$.

Proof:
($\Rightarrow$) Let $x \in U(Y)$, then there is $y$ s.t. $x = U(y)$. Then $U(L(x)) = U(L(U(y))) = U(y) = x$, ie, $x$ is a fixpoint of $U \circ L$.
($\Leftarrow$) Let $x = U(L(x))$, since $L(x) \in Y$, $x \in U(Y)$.

# Some Lemmas

Let $\langle X, \leq \rangle, \langle Y, \sqsubseteq \rangle, L, U$ be a GC.

Then
$U(Y) = U(L(X))$ and $L(X) = L(U(Y))$

Proof:
$(\subseteq)$ $x \in U(Y)$ iff $x = U(L(x))$, that is $x \in U(L(X))$.
$(\supseteq)$ $x \in U(L(X))$, then $x = U(y)$ for some $y \in L(X) \subseteq Y$. So $x \in U(Y)$.

# Finding Order Isomorphisms

Let $\langle X, \leq \rangle, \langle Y, \sqsubseteq \rangle, L, U$ be a GC.

Then
$\langle U(L(X)), \leq \rangle, \langle L(U(Y)), \sqsubseteq \rangle$ are order isomorphic.

Proof:
$\langle U(L(X)), \leq \rangle = \langle U(Y), \leq \rangle$ and $\langle L(U(Y)), \sqsubseteq \rangle = \langle L(X), \sqsubseteq \rangle$.
$L$ is the candidate isomorphism.
$L$ surjective onto $L(X)$ (from $U(Y)$): $y \in L(X)$ then $y = L(x)$ for some $x \in X$ then $y = L(U(L(x)))$. But $U(L(x)) \in U(Y)$.

# Finding Order Isomorphisms

Let $\langle X, \leq \rangle, \langle Y, \sqsubseteq \rangle, L, U$ be a GC.

Then
$\langle U(L(X)), \leq \rangle, \langle L(U(Y)), \sqsubseteq \rangle$ are order isomorphic.

Proof (contd):
$L$ is an order embedding: We already know $L$ is monotonic.
To prove: $L(x) \sqsubseteq L(x') \Rightarrow x \leq x'$.
Let $L(x) \sqsubseteq L(x')$, then $U(L(x)) \leq U(L(x'))$. But since $x, x' \in U(Y)$, $U(L(x)) = x$ and $U(L(x')) = x'$ and thus $x \leq x'$.