Galois 接続とプログラム解析

山口悠地

2025 年 7 月

目次

1 Galois 接続

1.1 定義

定義 1: Galois 接続

半順序集合 $(L, \leq_L)$ と $(M, \leq_M)$ と $\alpha : L \to M$ と $\gamma : M \to L$ が次の条件を満たすとき (L, α, γ, M) は **Galois 接続** であるという．

1. α, γ は単調．
2. 任意の $l \in L, m \in M$ に対して $l \leq_L \gamma(\alpha(l))$ かつ $\alpha(\gamma(m)) \leq_M m$．

■プログラム解析における Galois 接続の直感的な理解　ざっくり直感的な説明を述べる．

プログラム解析は，常にいくらでも具体的なものに対してできるとは限らない．

例えば以下のプログラムの終了時に `z` がとる値について何らかの解析を行うことを考える．

```
1  x = 1;
2  y = 2;
3  if rand()
4    z = x + y;
5  else
6    z = x - y;
7  end
```

最も理想的には値の集合: $\{-1, 3\}$ を解析結果として得たい．しかし，一般的にこのような具体的な値 (この例では $(= \mathcal{P}(\mathbb{Z}))$) を得るのは計算コストが高かったり，あるいはそもそも不可能であることが多い．

そこで，これまで見てきたように **ほどよい性質まで抽象化する**ことによって計算を可能にしてきた．例えば

- 偶奇のみを考える
- 区間のみを考える
- データ型のみを考える

などである．

Galois 接続はこのような抽象化と具体化の関係を表すものといえる．

定義における L が具体的な値の集合と対応し， M が抽象的な値の集合と対応する．つまり α は「抽象化」を行う関数，最も典型的にはプログラムの値の集合を抽象化した性質に写す関数である．そして γ は「具体化」を行う関数であり，抽象的な性質を具体的な値に写す．これらを使って解析を容易に行える抽象的な領域で解析を行うわけである．ここからは具体例および諸性質の理解を通して条件の確認・直感的な解釈を与える．

1.2 Galois 接続の例

整数のべき集合と整数の区間の間の Galois 接続を考えることができる．

$L = (\mathcal{P}(\mathbb{Z}), \subseteq)$, $M = (\mathbf{Interval}, \leq_i)$ とする.
(**Interval** の定義は **Example 4.10** を参照のこと.)
そして

$$\gamma(m) = \{z \in \mathbb{Z} \mid \inf(m) \leq z \leq \sup(m)\}$$
$$\alpha(l) = \begin{cases} \bot & \text{if } l = \emptyset \\ [\inf'(l), \sup'(l)] & \text{otherwise} \end{cases}$$

と定める.
例えば

- $\gamma([1,5]) = \{1,2,3,4,5\}$
- $\gamma([1,\infty)) = \{z \in \mathbb{Z} \mid z \geq 1\}$
- $\gamma(\bot) = \emptyset$
- $\alpha(\{1,2,3\}) = [1,3]$
- $\alpha(\{1,4,5\}) = [1,5]$
- $\alpha(\{2z \mid z > 0\}) = [-\infty, 0]$
- $\alpha(\emptyset) = \bot$

このとき, (L, α, γ, M) は Galois 接続である.
まず, γ の単調性: $m_1 \leq_i m_2 \implies \gamma(m_1) \subseteq \gamma(m_2)$ から確認する.

$$\begin{aligned} m_1 \leq_i m_2 &\implies \inf(m_2) \leq \inf(m_1) \wedge \sup(m_1) \leq \sup(m_2) && \text{(Definition of } \leq_i) \\ &\implies \forall z \in \{z \in \mathbb{Z} \mid \inf(m_1) \leq z \leq \sup(m_1)\}, z \in \{z \in \mathbb{Z} \mid \inf(m_2) \leq z \leq \sup(m_2)\} && \text{(Transitivity of } \leq) \\ &\implies \gamma(m_1) \subseteq \gamma(m_2) \end{aligned}$$

となり単調.
α の単調性: $l_1 \subseteq l_2 \implies \alpha(l_1) \leq_i \alpha(l_2)$ も確認しよう.

$$\begin{aligned} l_1 \subseteq l_2 &\implies \inf'(l_2) \leq \inf'(l_1) \wedge \sup'(l_1) \leq \sup'(l_2) \\ &\implies \alpha(l_1) \leq_i \alpha(l_2) \end{aligned}$$

より単調である.
続いて任意の $l \in L, m \in M$ に対して $l \subseteq \gamma(\alpha(l))$ かつ $\alpha(\gamma(m)) \leq_i m$ なることを示す.
まず $l \subseteq \gamma(\alpha(l))$ を示す.

- $l = \emptyset$ のとき: $\gamma(\alpha(l)) = \gamma(\bot) = \emptyset \subseteq l$.
- $l \neq \emptyset$ のとき:

$$\begin{aligned} \gamma(\alpha(l)) &= \gamma\left([\inf'(l), \sup'(l)]\right) \\ &= \{z \in \mathbb{Z} \mid \inf'(l) \leq z \leq \sup'(l)\} \\ &\supseteq \{z \in \mathbb{Z} \mid z \in l\} \\ &= l \end{aligned}$$

また $\alpha(\gamma(m)) \leq m$ は

- $m = \bot$ のとき $\alpha(\gamma(m)) = \alpha(\emptyset) = \bot \leq m$
- $m = [m_1, m_2] \neq \bot$ のとき:

$$\begin{aligned}\alpha(\gamma(m)) &= \alpha\left(\{z \in \mathbb{Z} \mid m_1 \leq z \leq m_2\}\right) \\ &= [m_1, m_2] \\ &= m \\ &\leq m\end{aligned}$$

よって (L, α, γ, M) は Galois 接続である.

1.3 随伴

定義 1 と同値な定義を使うと便利なことがある.

定義 2: 随伴

半順序集合 $(L, \leq_L)$ と $(M, \leq_M)$ について全域関数 $\alpha : L \to M$ と $\gamma : M \to L$ が次の条件を満たすとき (L, α, γ, M) を **随伴** であるという.

$$\alpha(l) \leq_M m \iff l \leq_L \gamma(m)$$

次が成り立つ.

定理 1: Galois 接続と随伴の関係

(L, α, γ, M) が Galois 接続のとき，またそのときに限り (L, α, γ, M) は随伴である.

■証明 ▷ **(Galois 接続 $\implies$ 随伴)**

$$\begin{aligned}\alpha(l) \leq_M m &\implies \gamma(\alpha(l)) \leq_L \gamma(m) && \text{(monotonicity of } \gamma) \\ &\implies l \leq_L \gamma(\alpha(l)) \leq_L \gamma(m) && \text{(definition of Galois connection)} \\ &\implies l \leq_L \gamma(m) && \text{(transitivity of } \leq_L)\end{aligned}$$

また

$$\begin{aligned}l \leq_L \gamma(m) &\implies \alpha(l) \leq_M \alpha(\gamma(m)) && \text{(monotonicity of } \alpha) \\ &\implies \alpha(l) \leq_M m \leq_M \alpha(\gamma(m)) && \text{(definition of Galois connection)} \\ &\implies \alpha(l) \leq_M m && \text{(transitivity of } \leq_M)\end{aligned}$$

▷ **(随伴 $\implies$ Galois 接続)**

まず条件 2 について示そう.
$l \in L$ に対して:

$$\begin{aligned} & l \leq_L l && \text{(reflexivity of } \leq_L) \\ & \alpha(l) \leq_M \alpha(l) && \text{(reflexivity of } \leq_M) \\ & \implies l \leq_L \gamma(\alpha(l)) && \text{(assumption: } \alpha(l) \leq_M m \implies l \leq_L \gamma(m)) \end{aligned}$$

となり, $l \leq_L \gamma(\alpha(l))$ が成立.
同様に, $m \in M$ に対して:

$$\begin{aligned} & m \leq_M m && \text{(reflexivity of } \leq_M) \\ & \gamma(m) \leq_L \gamma(m) && \text{(reflexivity of } \leq_L) \\ & \implies \alpha(\gamma(m)) \leq_M m && \text{(assumption: } l \leq_L \gamma(m) \implies \alpha(l) \leq_M m) \end{aligned}$$

で, $\alpha(\gamma(m)) \leq_M m$ となる.
続いて, 条件 1 (単調性) を示す.
α の単調性: $l_1 \leq_L l_2$ のとき $\alpha(l_1) \leq_M \alpha(l_2)$ は

$$\begin{aligned} l_1 \leq_L l_2 & \implies l_1 \leq_L l_2 \leq_L \gamma(\alpha(l_2)) && (l \leq_L \gamma(\alpha(l))) \\ & \implies \alpha(l_1) \leq_M \alpha(l_2) && \text{(assumption: } \alpha(l) \leq_M m \implies l \leq_L \gamma(m)) \end{aligned}$$

となりしたがう.
同様に γ の単調性: $m_1 \leq_M m_2$ のとき $\gamma(m_1) \leq_L \gamma(m_2)$ は

$$\begin{aligned} m_1 \leq_M m_2 & \implies m_1 \leq_M m_2 \leq_M \alpha(\gamma(m_2)) && (m \leq_M \alpha(\gamma(m))) \\ & \implies \gamma(m_1) \leq_L \gamma(m_2) && \text{(assumption: } l \leq_L \gamma(m) \implies \alpha(l) \leq_M m) \end{aligned}$$

□

1.4 Galois 接続と Representation Function

集合 V と 完備束 $(L, \leq_L)$ について Repersentation Function $\beta : V \to L$ から Galois 接続を構成することができる.

定理 2: Representation Function と Galois 接続

集合 V， 完備束 $(L, \leq_L)$ と $\beta : V \to L$ について
$\alpha : \mathcal{P}(V) \to L$ と $\gamma : L \to \mathcal{P}(V)$ を次のように定義する．

$$\alpha(V') = \bigsqcup_{v \in V'} \beta(v)$$
$$\gamma(l) = \{v \in V \mid \beta(v) \leq_L l\}$$

このとき $(\mathcal{P}(V), \subseteq)$, $(L, \leq_L)$ は半順序であって，$(L, \alpha, \gamma, \mathcal{P}(V))$ は Galois 接続である．

■証明　随伴であることを示すことにより Galois 接続であることを示す．

$(L, \leq_L)$ は完備束なので α は全域関数．また， Representation Function なので β は全域．したがって γ も全域なことがしたがう．

そして

$$\begin{aligned}
\alpha(V') \leq_L l &\iff \bigsqcup_{v \in V'} \beta(v) \leq_L l && \text{(definition of } \alpha\text{)} \\
&\iff \forall v \in V', \beta(v) \leq_L l && \text{(property of } \textstyle\bigsqcup\text{)} \\
&\iff V' \subseteq \gamma(l) && \text{(definition of } \gamma\text{)}
\end{aligned}$$

よって 定理 1 より $(\mathcal{P}(V), \alpha, \gamma, L)$ は Galois 接続である．

□

1.4.1 extraction function

とくに **extraction function** という例を考えることができる．

集合 V, D と $\eta : V \to D$ を考える．V, D はとくに半順序集合などに限定されていないことに注意せよ．

定理 2 において

$$\begin{aligned}
V &\leftarrow V \\
L &\leftarrow \mathcal{P}(D) \\
\leq_L &\leftarrow \subseteq \\
\beta &\leftarrow v \mapsto \{\eta(v)\}
\end{aligned}$$

とすると 半順序集合 $(\mathcal{P}(V), \subseteq)$ と $(\mathcal{P}(D), \subseteq)$ は

$$\begin{aligned}
\alpha(V') &= \bigcup_{v \in V'} \{\eta(v)\} \\
&= \{\eta(v) \mid v \in V'\} \\
\gamma(D') &= \{v \in V \mid \eta(v) \in D'\}
\end{aligned}$$

によって Galois 接続 $(\mathcal{P}(V), \alpha, \gamma, \mathcal{P}(D))$ をなすことがわかる.
この値 v を抽象的な記述 d に写す η を *extraction function* と呼ぶ.
実際の問題の例で考えよう.
$V = \mathbb{Z}$, $D = \{-, 0, +\}$ として
$\mathrm{sign} : \mathbb{Z} \to D$ を次のように定義する.

$$\mathrm{sign}(z) = \begin{cases} - & \text{if } z < 0 \\ 0 & \text{if } z = 0 \\ + & \text{if } z > 0 \end{cases}$$

と定める.
このとき, 先ほどの議論から

$$\alpha_{\mathrm{sign}}(V') = \{\mathrm{sign}(v) \mid z \in V'\}$$
$$\gamma_{\mathrm{sign}}(D') = \{z \in \mathbb{Z} \mid \mathrm{sign}(z) \in D'\}$$

とすると $(\mathcal{P}(\mathbb{Z}), \alpha_{\mathrm{sign}}, \gamma_{\mathrm{sign}}, \mathcal{P}(D))$ は Galois 接続.
実際に計算例を見ると:

$$\alpha_{\mathrm{sign}}(\{-1\}) = \{\mathrm{sign}(-1)\} = \{-\}$$
$$\alpha_{\mathrm{sign}}(\{-1, 0, 1\}) = \{\mathrm{sign}(-1), \mathrm{sign}(0), \mathrm{sign}(1)\} = \{-, 0, +\}$$
$$\alpha_{\mathrm{sign}}(\{-2, 0, 3, 4\}) = \{\mathrm{sign}(-2), \mathrm{sign}(0), \mathrm{sign}(3)\} = \{-, 0, +\}$$
$$\gamma_{\mathrm{sign}}(\{-\}) = \{z \in \mathbb{Z} \mid \mathrm{sign}(z) = -\} = \{z \in \mathbb{Z} \mid z < 0\}$$
$$\gamma_{\mathrm{sign}}(\{-, 0\}) = \{z \in \mathbb{Z} \mid \mathrm{sign}(z) = - \vee \mathrm{sign}(z) = 0\} = \{z \in \mathbb{Z} \mid z \leq 0\}$$

1.5 Galois 接続の性質

定理 3

半順序集合 $(L, \leq_L)$ と $(M, \leq_M)$ と $\alpha : L \to M$ と $\gamma : M \to L$ が Galois 接続 (L, α, γ, M) をなすとき

$$\alpha \circ \gamma \circ \alpha = \alpha$$
$$\gamma \circ \alpha \circ \gamma = \gamma$$

■証明

$$\begin{aligned} & l \leq_L \gamma(\alpha(l)) && \text{(Definition of Galois connection)} \\ \Longrightarrow\ & \alpha(l) \leq_M \alpha(\gamma(\alpha(l))) && \text{(Monotonicity of } \alpha\text{)} \end{aligned}$$

また

$$\begin{aligned} & \gamma(\alpha(l)) \leq_L \gamma(\alpha(l)) && \text{(Reflexivity of } \leq_L) \\ \Longrightarrow\ & \alpha(\gamma(\alpha(l))) \leq_M \alpha(l) && \text{(Theorem 1)} \end{aligned}$$

なので $\leq_M$ の反対称性から $\alpha(l) = \alpha(\gamma(\alpha(l)))$
同様に

$$\begin{aligned} & \alpha(\gamma(m)) \leq_M m && \text{(Definition of Galois connection)} \\ \Longrightarrow\ & \gamma(m) \leq_L \gamma(\alpha(\gamma(m))) && \text{(Monotonicity of } \gamma) \end{aligned}$$

また

$$\begin{aligned} & \alpha(\gamma(m)) \leq_M \alpha(\gamma(m)) && \text{(Reflexivity of } \leq_M) \\ \Longrightarrow\ & \gamma(\alpha(\gamma(m))) \leq_L \gamma(m) && \text{(Theorem 1)} \end{aligned}$$

となり $\leq_L$ の反対称性から $\gamma(m) = \gamma(\alpha(\gamma(m)))$.

□

補題 1: α の上界の保存性

完備束 $(L, \leq_L)$, $(M, \leq_M)$ と $\alpha : L \to M$ について Galois 接続 (L, α, γ, M) が存在するとき，任意の $L' \subseteq L$, $m \in M$ について

$$\alpha\left(\bigsqcup_{l \in L'} l\right) \leq_M m \iff \bigsqcup_{l \in L'} \alpha(l) \leq_M m$$

■証明

$$\begin{aligned} \alpha\left(\bigsqcup_{l \in L'} l\right) \leq_M m &\iff \bigsqcup_{l \in L'} l \leq_L \gamma(m) && \text{(Theorem 1)} \\ &\iff \forall l \in L', l \leq_L \gamma(m) && \text{(property of } \textstyle\bigsqcup) \\ &\iff \forall l \in L', \alpha(l) \leq_M m && \text{(Theorem 1)} \\ &\iff \bigsqcup_{l \in L'} \alpha(l) \leq_M m \end{aligned}$$

□

ここから次の性質が従う.

補題 2: α の完全加法性

完備束 $(L, \leq_L)$, $(M, \leq_M)$ と $\alpha : L \to M$ について Galois 接続 (L, α, γ, M) が存在するとき， α は完全加法的である．すなわち，任意の $L' \subseteq L$ について

$$\alpha\left(\bigsqcup_{l \in L'} l\right) = \bigsqcup_{l \in L'} \alpha(l)$$

■証明　補題 1 において，とくに $m \leftarrow \bigsqcup_{l \in L'} \alpha(l)$ と $m \leftarrow \alpha\left(\bigsqcup_{l \in L'} l\right)$ とすると $\leq_M$ の反対称性からしたがう．

これらの補題から，以下の重要な性質を得ることができる．

定理 4: α による γ の決定

完備束 $(L, \leq_L)$, $(M, \leq_M)$, $\alpha : L \to M$ について Galois 接続 (L, α, γ, M) が存在するとき γ は

$$\gamma(m) = \bigsqcup\{l \in L \mid \alpha(l) \leq_M m\}$$

によって一意に定まる．

■証明　▷ **(一意性)**

γ_1, γ_2 が Galois 接続 (L, α, γ_1, M) と (L, α, γ_2, M) をなすとき， $\gamma_1 = \gamma_2$ であることを示す．
Galois 接続の定義から

$$\alpha(\gamma_1(m)) \leq_M m \tag{1}$$
$$\alpha(\gamma_2(m)) \leq_M m \tag{2}$$

定理 1 を (1) に対して $\gamma \leftarrow \gamma_2$, (2) に対して $\gamma \leftarrow \gamma_1$ として使うと

$$\gamma_1(m) \leq_M \gamma_2(m)$$
$$\gamma_2(m) \leq_M \gamma_1(m)$$

となり $\gamma_1(m) = \gamma_2(m)$ がしたがう．

▷ **(γ の正当性)**

$\gamma(m) = \bigsqcup\{l \in L \mid \alpha(l) \leq_M m\}$ が条件:

1. 単調性
2. 任意の $l \in L, m \in M$ に対して $l \leq_L \gamma(\alpha(l))$ かつ $\alpha(\gamma(m)) \leq_M m$

なることを示す.
まず単調性:
$m_1 \leq_M m_2 \implies \gamma(m_1) \leq_M \gamma(m_2)$ を示す.
$m_1 \leq_M m_2$ のとき, $\leq_M$ が推移的であることに注意すれば

$$\{l \in L \mid \alpha(l) \leq_M m_1\} \subseteq \{l \in L \mid \alpha(l) \leq_M m_2\}$$

さらに
$(M, \leq_M)$ の $\bigsqcup$ の性質: $a \subseteq b \implies \bigsqcup a \leq_M \bigsqcup b$ を使うと

$$\gamma(m_1) = \bigsqcup\{l \in L \mid \alpha(l) \leq_M m_1\} \leq_M \bigsqcup\{l \in L \mid \alpha(l) \leq_M m_2\} = \gamma(m_2)$$

となって単調性がしたがう.
続いて, 任意の $l \in L, m \in M$ に対して $l \leq_L \gamma(\alpha(l))$ かつ $\alpha(\gamma(m)) \leq_M m$ なることを示す.
まず $l \leq_L \gamma(\alpha(l))$ は

$$\gamma(\alpha(l)) = \bigsqcup\{l' \in L \mid \alpha(l') \leq_M \alpha(l)\} \ni l$$

よって $\bigsqcup$ の定義から $l \leq_L \gamma(\alpha(l))$ がしたがう.
つぎに $\alpha(\gamma(m)) \leq_M m$ を示す.

$$\begin{aligned} & \bigsqcup\{\alpha(l) \mid l \in L, \alpha(l) \leq_M m\} \leq_M m && \text{(Property of } \textstyle\bigsqcup\text{)} \\ \iff & \gamma(m) = \alpha(\bigsqcup\{l \in L \mid \alpha(l) \leq_M m\}) \leq_M m && \text{(Lemma 1)} \end{aligned}$$

以上から $\gamma(m) = \bigsqcup\{l \in L \mid \alpha(l) \leq_M m\}$ によって一意に γ が定まり (L, α, γ, M) は Galois 接続.

□

同様の議論によって次の事実も得られる.

定理 5: γ の完全乗法性

完備束 $(L, \leq_L)$, $(M, \leq_M)$ と $\gamma : M \to L$ について Galois 接続 (L, α, γ, M) が存在するとき, γ は完全乗法的である. すなわち, 任意の $M' \subseteq M$ について

$$\gamma\left(\prod_{m \in M'} m\right) = \prod_{m \in M'} \gamma(m)$$

定理 6: γ による α の決定

完備束 $(L, \leq_L)$, $(M, \leq_M)$, $\gamma : M \to L$ について Galois 接続 (L, α, γ, M) が存在するとき α は

$$\alpha(l) = \bigsqcup\{m \in M \mid l \leq_L \gamma(m)\}$$

によって一意に定まる.

さらに，補題 2 の逆も成立する.

定理 7: 完全加法性と Galois 接続の存在条件

完備束 $(L, \leq_L)$, $(M, \leq_M)$ と $\alpha : L \to M$ について α が完全加法的であるとき， Galois 接続 (L, α, γ, M) が存在する.

■証明 $\gamma : M \to L$ を $\gamma(m) = \bigsqcup\{l \in L \mid \alpha(l) \leq_M m\}$ によって定めて，これが Galois 接続 (L, α, γ, M) をなすことを示す.

まず α の単調性を示そう． $l_1 \leq_L l_2$ のとき

$$\begin{aligned}
\alpha(l_2) &= \alpha(\bigsqcup\{l_1, l_2\}) \\
&= \bigsqcup\{\alpha(l_1), \alpha(l_2)\} && \text{(Complete additivity of } \alpha\text{)} \\
&\geq_M \alpha(l_1) && \text{(Property of } \bigsqcup\text{)}
\end{aligned}$$

γ の単調性と $l \in L$ に対して $l \leq_L \gamma(\alpha(l))$ であることは定理 4 と同様に示せる.
あとは任意の $m \in M$ に対して $\alpha(\gamma(m)) \leq_M m$ なることを示せばよい.
$l \in L, m \in M$ に対して

$$\begin{aligned}
\alpha(\gamma(m)) &= \alpha\left(\bigsqcup\{l' \in L \mid \alpha(l') \leq_M m\}\right) && \text{(Definition of } \gamma\text{)} \\
&= \bigsqcup\{\alpha(l') \mid l' \in L, \alpha(l') \leq_M m\} && \text{(Complete additivity of } \alpha\text{)} \\
&\leq_M m
\end{aligned}$$

したがって (L, α, γ, M) は Galois 接続である.

□

同様の議論によって次も成立する.

定理 8: 完全乗法性と Galois 接続の存在条件

完備束 $(L, \leq_L)$, $(M, \leq_M)$ と $\gamma : M \to L$ について γ が完全乗法的であるとき， Galois 接続 (L, α, γ, M) が存在する.

1.6 正当性関係との関係

4.10 節で議論した正当性関係 R は以下のようなものであった.
値 V と 性質 L の二項関係であって, $v \in V, l_1, l_2 \in L, L' \subseteq L$ に対して

$$v\ R\ l_1 \wedge l_1 \sqsubseteq l_2 \implies v\ R\ l_2 \tag{3}$$
$$\forall l' \in L', v\ R\ l' \implies v\ R\ \left(\bigsqcup L'\right) \tag{4}$$

ここで, より抽象的な領域 M についてこの正当性関係をどう扱えるかを考察する.
次のように V と M の二項関係 S を定義する.

定義 3: 抽象領域における正当性関係

Galois 接続 (L, α, γ, M) が与えられたとき, V, M の二項関係 S を次のように定義する. $v \in V, m \in M$ に対して

$$v\ S\ m \iff v\ R\ \gamma(m)$$

このとき, S **もまた正当性関係** である.

定理 9: Galois 接続と正当性関係

S は正当性関係である. すなわち, $v \in V, m_1, m_2 \in M, M' \subseteq M$ に対して

$$v\ S\ m_1 \wedge m_1 \leq_M m_2 \implies v\ S\ m_2 \tag{5}$$
$$\forall m \in M', v\ S\ m \implies v\ S\ \left(\bigsqcap M'\right) \tag{6}$$

(5):

$$\begin{aligned}
v\ S\ m_1 \wedge m_1 \leq_M m_2 &\implies v\ R\ \gamma(m_1) \wedge \gamma(m_1) \leq_L \gamma(m_2) && \text{(Definition of } S\text{, monotonicity of } \gamma) \\
&\implies v\ R\ \gamma(m_2) && (3) \\
&\implies v\ S\ m_2 && \text{(Definition of } S)
\end{aligned}$$

(6):

$$\begin{aligned}
\forall m \in M', v\ S\ m &\implies \forall m \in M', v\ R\ \gamma(m) && \text{(Definition of } S) \\
&\implies v\ R\ \left(\bigsqcap_{m \in M'} \gamma(m)\right) && \text{(Definition of } R\text{: } v\ R\ l_1 \wedge l_1 \sqsubseteq l_2 \implies v\ R\ l_2) \\
&\implies v\ R\ \gamma\left(\bigsqcap M'\right) && \text{(Complete multiplicativity of } \gamma) \\
&\implies v\ S\ \left(\bigsqcap M'\right) && \text{(Definition of } S)
\end{aligned}$$

1.7 Galois 挿入

ここまで， Galois 接続がプログラム解析の正当性を保ったまま適切に抽象化するような構造であることを見てきた．ここでは， Galois 接続のうち **Galois 挿入** (Galois insertion) と呼ばれるものの定義と具体例，性質について見ていく．

定義 4: Galois 挿入

(L, α, γ, M) が Galois 接続であって，

$$\alpha \circ \gamma = \mathrm{id}_M$$

であるとき (L, α, γ, M) が **Galois 挿入** (Galois insertion) であるという．

このような (L, α, γ, M) は，存在する．
たとえば 1.2 節で紹介した

$$\begin{aligned} L &= (\mathcal{P}(\mathbb{Z}), \subseteq) \\ M &= (\mathbf{Interval}, \leq_i) \\ \alpha(l) &= \begin{cases} \bot & \text{if } l = \emptyset \\ [\inf'(l), \sup'(l)] & \text{otherwise} \end{cases} \\ \gamma(m) &= \{z \in \mathbb{Z} \mid \inf(m) \leq z \leq \sup(m)\} \end{aligned}$$

は Galois 挿入である．
Galois 接続であって Galois 挿入でないものも存在する．

$$\begin{aligned} V &= \mathbb{Z} \\ D &= \mathbf{Sign} \times \mathbf{Parity} \end{aligned}$$

とする．ここで， extraction function $\eta : V \to D$ を

$$\eta(z) = (\mathrm{sign}(z), \mathrm{parity}(z))$$

によって定めれば，

$$\begin{aligned} L &= (\mathcal{P}(V), \subseteq) \\ M &= (\mathcal{P}(D), \subseteq) \\ \alpha(V') &= \{(\mathrm{sign}(v), \mathrm{parity}(v)) \mid v \in V'\} \\ \gamma(D') &= \{v \in V \mid (\mathrm{sign}(v), \mathrm{parity}(v)) \in D'\} \end{aligned}$$

は Galois 接続 (L, α, γ, M) をなす．

しかし $\{(0, odd)\} \in M$ に対して

$$\begin{aligned}\alpha(\gamma(\{(0, odd)\})) &= \alpha(\emptyset) \\ &= \emptyset \\ &\neq \{(0, odd)\}\end{aligned}$$

なので，(L, α, γ, M) は Galois 挿入ではない.

1.7.1 Galois 挿入の直感的な理解

二つ目の例では，対応する具体的な値がないような「余分な」抽象領域の存在によって Galois 挿入とならなかった．Galois 挿入は，このような「余分な」抽象領域が存在しないような Galois 接続であると直感的に理解できる．そのことをはっきり示すような諸性質を以下に示す.

1.7.2 Galois 挿入の性質

Galois 挿入 (L, α, γ, M) について，以下の性質が成り立つ.

定理 10: Galois 挿入の性質

Galois 接続 (L, α, γ, M) について，以下は同値.

i. (L, α, γ, M) が Galois 挿入
ii. γ が単射
iii. α が全射
iv. γ は順序を保存する: $\forall m_1, m_2 \in M, \gamma(m_1) \leq_L \gamma(m_2) \implies m_1 \leq_M m_2$

■証明 ▷ **(i) $\implies$ (ii)**

$m_1, m_2 \in M$ に対して,

$$\begin{aligned}\gamma(m_1) = \gamma(m_2) &\implies \alpha(\gamma(m_1)) = \alpha(\gamma(m_2)) \\ &\implies m_1 = m_2 \qquad \text{(Definition of Galois insertion)}\end{aligned}$$

よって γ は単射である.

▷ **(ii) $\implies$ (iii)**

$m \in M$ に対して, 定理 3 から $\gamma(\alpha(\gamma(m))) = \gamma(m)$. ここで γ の単射性から $\alpha(\gamma(m)) = m$ がしたがう. したがって各 $m \in M$ に対して $l\ (= \gamma(m))$ が存在して $\alpha(l) = m$ となるので α は全射である.

▷ **(iii) $\implies$ (iv)**

$m_1 \leq_M m_2 \implies \gamma(m_1) \leq_L \gamma(m_2)$ は γ の単調性からただちにしたがう.
$\gamma(m_1) \leq_L \gamma(m_2) \implies m_1 \leq_M m_2$ を示そう.
仮定 (iii) から $\alpha(l_1) = m_1$, $\alpha(l_2) = m_2$ なるような $l_1, l_2 \in L$ が存在する. 定理 1 を $l \leftarrow l_1, m \leftarrow m_1$ として使うと

$$\alpha(l_1) = m_1 \leq_M m_1 \iff l_1 \leq_L \gamma(m_1)$$

よって $\leq_L$ の推移性から

$$\gamma(m_1) \leq_L \gamma(m_2) \implies l_1 \leq_L \gamma(m_2)$$

ここで $l_1 \leq_L \gamma(m_2)$ に対してもふたたび 定理 1 を $l \leftarrow l_1, m \leftarrow m_2$ として使うと

$$l_1 \leq_L \gamma(m_2) \iff \alpha(l_1) \leq_M m_2 \iff m_1 \leq_M m_2$$

なので, 結局 $\gamma(m_1) \leq_L \gamma(m_2) \implies m_1 \leq_M m_2$.

▷ **(iv) $\implies$ (i)**

$$\begin{aligned} \alpha(\gamma(m_1)) \leq_M m_2 &\iff \gamma(m_1) \leq_L \gamma(m_2) && \text{(Theorem 1)} \\ &\iff m_1 \leq_M m_2 && \text{(Assumption of (iv))} \end{aligned}$$

よってとくに $m2 \leftarrow \alpha(\gamma(m_1))$, $m_1 \leftarrow m_2$ を考えれば

$$\alpha(\gamma(m_1)) = m_1$$

がしたがう.

これらから (i) $\iff$ (ii) $\iff$ (iii) $\iff$ (iv) が成り立つことがわかる.

□

1.8 reduction operator による Galois 挿入の構成

先ほど示したような条件を満たすような Galois 接続が Galois 挿入であることがわかった. ではこれらの条件を満たすように Galois 接続から Galois 挿入を構成することはできるだろうか?

直感的には,「余分な」抽象領域を削除すれば構成できそうである. つまり:

予想 1: reduction operator による Galois 挿入の構成

完備束 $(L, \leq_L)$, $(M, \leq_M)$ と $\alpha : L \to M$ が Galois 接続 (L, α, γ, M) をなすとき $\varsigma : M \to M$ を

$$\varsigma(m) = \bigsqcap \{m' \mid \gamma(m') = \gamma(m)\}$$

と定める. このとき

$\varsigma[M] = (\{\varsigma(m) \mid m \in M\}, \leq_M)$ は完備束であり，$(L, \alpha, \gamma, \varsigma[M])$ は Galois 挿入をなす．

■例

$$
\begin{aligned}
L &= (\mathcal{P}(\mathbb{Z}), \subseteq) \\
M &= (\mathcal{P}(\mathbf{Sign} \times \mathbf{Parity}), \subseteq) \\
\alpha(V') &= \{(\mathrm{sign}(v), \mathrm{parity}(v)) \mid v \in V'\} \\
\gamma(D') &= \{v \in V \mid (\mathrm{sign}(v), \mathrm{parity}(v)) \in D'\}
\end{aligned}
$$

について，
$\varsigma : M \to M$ は

$$\varsigma(m) = \bigcap \{m' \in M \mid \gamma(m') = \gamma(m)\}$$

例えば:

$$
\begin{aligned}
\varsigma(\{(+, even)\}) &= \bigcap \{m' \in M \mid \gamma(m') = \{2, 4, 6, \ldots\}\} \\
&= \bigcap \{\{(+, even)\}\} \\
&= \{(+, even)\}
\end{aligned}
$$

$$
\begin{aligned}
\varsigma(\{(+, even), (+, odd)\}) &= \bigcap \{m' \in M \mid \gamma(m') = \{1, 2, 3, \ldots\}\} \\
&= \bigcap \{\{(+, even), (+, odd)\}, \{(+, even), (+, odd), (0, even)\}\} \\
&= \{(+, even), (+, odd)\}
\end{aligned}
$$

定義から $\gamma(\{S\}) = \emptyset$ になるような S について，$\gamma(V \cap S) = \gamma(V)$ が成り立つ．しかし，最後の例にとくに注目すると，そのような S が共通部分を取ることで「落とされ」るように働いていることがわかる．

そして，**実際このような変換によって Galois 挿入が得られる．**ここからはそれを示していく．

補題 3: $\alpha[L]$ と $(\mathbf{Fix}(\alpha \circ \gamma), \leq_M)$ の一致

完備束 $(L, \leq_L)$, $(M, \leq_M)$ と $\alpha : L \to M$ が Galois 接続 (L, α, γ, M) をなすとき

$$\alpha[L] = (\{\alpha(l) \mid l \in L\}, \leq_M)$$

と定める．このとき

$$\alpha[L] = (\mathrm{Fix}(\alpha \circ \gamma), \leq_M)$$

■証明　▷ **($\alpha[L] \subseteq \mathbf{Fix}(\alpha \circ \gamma)$)**

$m \in \alpha[L]$ をとる．$m = \alpha(l)$ なる $l \in L$ が存在するので，$\alpha(\gamma(m)) = \alpha(\gamma(\alpha(l)))$ とすることができる．
$\alpha(\gamma(\alpha(l))) = \alpha(l)$ なので結局 $\alpha(\gamma(m)) = m$ となり $m \in \mathrm{Fix}(\alpha \circ \gamma)$.

▷ **($\mathbf{Fix}(\alpha \circ \gamma) \subseteq \alpha[L]$)**

$m \in \mathrm{Fix}(\alpha \circ \gamma)$ をとる．$\alpha(\gamma(m)) = m$ なので，$l = \gamma(m)$ なる l が $\alpha(l) = m$ となり $m \in \alpha[L]$.

□

補題 4: $\alpha \circ \gamma$ と ς の一致

完備束 $(L, \leq_L)$, $(M, \leq_M)$ と $\alpha : L \to M$, $\gamma : M \to L$ が Galois 接続 (L, α, γ, M) をなすとき reduction operator $\varsigma(m) = \bigsqcap\{m' \in M \mid \gamma(m') = \gamma(m)\}$ は $\alpha \circ \gamma$ と一致する．

■証明　$S(m) = \{m' \in M \mid \gamma(m') = \gamma(m)\}$ とする．
このとき

▷ **$\alpha(\gamma(m))$ は S の下界である**

$s \in S(m)$ に対して

$$\begin{aligned} \gamma(s) = \gamma(m) &\implies \gamma(s) \leq_L \gamma(m) && \text{(Reflexivity of } \leq_L) \\ &\implies \alpha(\gamma(m)) \leq_M s && \text{(Theorem 1)} \end{aligned}$$

定義から任意の $s \in S(m)$ について $\gamma(s) = \gamma(m)$ なので，$\alpha(\gamma(m))$ は $S(m)$ の下界である．

▷ **$\alpha(\gamma(m))$ は下界の中で最大**

S の下界 $m' \in M$ をとる．定義から 任意の $s \in S(m)$ に対して $m' \leq_M s$.
そして

$$\begin{aligned} m' \leq_M s &\implies \gamma(m') \leq_L \gamma(s) && \text{(Monotonicity of } \gamma) \\ &\implies \gamma(m') \leq_L \gamma(m) && \text{(Definition of } S) \\ &\implies m' \leq_M \alpha(\gamma(m)) && \text{(Theorem 1)} \end{aligned}$$

したがって 任意の下界 $m' \in M$ に対して $m' \leq_M \alpha(\gamma(m))$ なので $\alpha(\gamma(m'))$ は $S(m)$ の下界の中で最大である．

これらから $\alpha(\gamma(m)) = \bigsqcap S(m) = \varsigma(m)$.

□

補題 5: $\alpha[L]$ と $\varsigma[M]$ の一致

完備束 $(L, \leq_L)$, $(M, \leq_M)$ と $\alpha : L \to M$, $\gamma : M \to L$ が Galois 接続 (L, α, γ, M) をなすとき $\alpha[L]$ と $\varsigma[M]$ は一致する.

■証明 ▷ $\varsigma[M] \subseteq \alpha[L]$

$\varsigma(m) = \alpha(\gamma(m))$ なので $l = \gamma(m)$ なる l が $\alpha(l) = m$ となり $m \in \alpha[L]$.

▷ $\alpha[L] \subseteq \varsigma[M]$

$\alpha[L] = \mathrm{Fix}(\alpha \circ \gamma)$ なので $m \in \alpha[L]$ をとると $\varsigma(m) = m$. よって $m \in \varsigma[M]$.

これら 3 つの補題から次の重要な事実が得られる.

定理 11: $\alpha[L]$, $\varsigma[M]$ は完備束

$\alpha[L]$ と $\varsigma[M]$ は完備束である.

■証明 $\alpha \circ \gamma$ は単調関数の合成であるから M 上の単調関数. したがって Knaster-Tarski の定理により $\mathrm{Fix}(\alpha \circ \gamma)$ は完備束をなし, 補題 4, 5 により $\alpha[L]$, $\varsigma[M]$ も完備束となる.

定理 12: reduction operator による Galois 挿入の構成

完備束 $(L, \leq_L)$, $(M, \leq_M)$ と $\alpha : L \to M$ が Galois 接続 (L, α, γ, M) をなすとき $\varsigma : M \to M$ を

$$\varsigma(m) = \bigsqcap \{m' \mid \gamma(m') = \gamma(m)\}$$

と定める. このとき
$\varsigma[M] = (\{\varsigma(m) \mid m \in M\}, \leq_M)$ は完備束であり, $(L, \alpha, \gamma, \varsigma[M])$ は Galois 挿入をなす.

■証明 定理 11 から $\varsigma[M]$ は完備束である.
$(L, \alpha, \gamma, \alpha[L])$ が Galois 挿入であることから $(L, \alpha, \gamma, \varsigma[M])$ が Galois 挿入であることを示す.
$\alpha[L] \subseteq M$ なので $(L, \alpha, \gamma, \alpha[L])$ は Galois 接続であることを保つ.
さらに, $\alpha[L]$ の定義から α は全射である. よって定理 10 により $(L, \alpha, \gamma, \alpha[L])$ は Galois 挿入をなす.
よって $(L, \alpha, \gamma, \varsigma[M])$ も Galois 挿入である.

□

1.9 extraction function によって定まる reduction operator

extraction function $\eta : V \to D$ が与えられたとき， reduction operator $\varsigma : M \to M$ がどのように定まるかを考察する．集合 V, D と extraction function $\eta : V \to D$ が与えられたとき，extraction function η によって定まる Galois 接続 $(L, \alpha_\eta, \gamma_\eta, M)$ を構成することができる．

このとき， reduction operator $\varsigma_\eta : M \to M$ は

$$\begin{aligned}\varsigma_\eta(D') &= \alpha(\gamma(D')) \\ &= \alpha\left(\{v \in V \mid \eta(v) \in D'\}\right) \\ &= \{\eta(v) \mid v \in V, \eta(v) \in D'\} \\ &= D' \cap \eta[V]\end{aligned}$$

となる．D のうち具体的な値によって記述されることがない部分を削除していることがわかる．

2 プログラム解析のための Galois 接続のシステマティックな構成

2.1 段階的な設計の構築

`https://abap34.github.io/Galois-Connections-in-Program-Analysis/`

2.2 環境，意味論の抽象化

定理 13: S から L, M への写像全体がなす **Galois 接続**

Galois 接続 (L, α, γ, M) と 集合 S に対して，$\alpha' : (S \to L) \to (S \to M)$,$\gamma' : (S \to M) \to (S \to L)$ を

$$\begin{aligned}\alpha'(f) &= \alpha \circ f \\ \gamma'(g) &= \gamma \circ g\end{aligned}$$

$S \to L$ と $S \to M$ 上 の順序 $\leq_{S\to L}, \leq_{S\to M}$ を

$$\begin{aligned}f \leq_{S\to L} f' &\iff \forall s \in S, f(s) \leq_L f'(s) \\ g \leq_{S\to M} g' &\iff \forall s \in S, g(s) \leq_M g'(s)\end{aligned}$$

によって定めれば $(S \to L, \leq_{S\to L})$ と $(S \to M, \leq_{S\to M})$ は半順序であって $(S \to L, \alpha', \gamma', S \to M)$ は Galois 接続.

■証明 α', γ' は全域.

$f \in S \to L, g \in S \to M$ に対して

$$
\begin{aligned}
\alpha'(f) \leq_{S\to M} g &\iff \forall s \in S, \alpha(f(s)) \leq_M g(s) && \text{(Definition of } \leq_{S\to M}) \\
&\iff \forall s \in S, f(s) \leq_L \gamma(g(s)) && (\ (L,\alpha,\gamma,M) \text{ is Galois connection}) \\
&\iff f \leq_{S\to L} \gamma'(g) && \text{(Definition of } \leq_{S\to L})
\end{aligned}
$$

より， 1 から $(S \to L, \alpha', \gamma', S \to M)$ は Galois 接続.

定理 14: Galois 接続間の単調関数がなす Galois 接続

Galois 接続 $(L_1, \alpha_1, \gamma_1, M_1)$ と $(L_2, \alpha_2, \gamma_2, M_2)$ に対して
$\mathcal{F}_L$ を $L_1 \to L_2$ の単調写像全体の集合，$\mathcal{F}_M$ を $M_1 \to M_2$ の単調写像全体の集合として，$\alpha : \mathcal{F}_L \to \mathcal{F}_M, \gamma : \mathcal{F}_M \to \mathcal{F}_L$ を

$$
\begin{aligned}
\alpha(f) &= \alpha_2 \circ f \circ \gamma_1 \\
\gamma(g) &= \gamma_2 \circ g \circ \alpha_1
\end{aligned}
$$

と定めたとき $(\mathcal{F}_L, \alpha, \gamma, \mathcal{F}_M)$ は Galois 接続.

■証明 α_1, γ_1, α_2, γ_2 の単調性から α, γ も単調.
$l_1 \in L_1$, $f \in \mathcal{F}_L$ に対して

$$
\begin{aligned}
& l_1 \leq_{L_1} \gamma_1(\alpha_1(l_1)) && ((L_1,\alpha_1,\gamma_1,M_1) \text{ is Galois connection}) \\
\implies\ & f(l_1) \leq_{L_2} f(\gamma_1(\alpha_1(l_1))) && \text{(Monotonicity of } f) \\
& \leq_{L_2} \gamma_2(\alpha_2(f(\gamma_1(\alpha_1(l_1))))) && ((L_2,\alpha_2,\gamma_2,M_2) \text{ is Galois connection})
\end{aligned}
$$

よって $\forall f \in \mathcal{F}_L, f \leq_{\mathcal{F}_L} \gamma(\alpha(f))$.
同様に,
$m_1 \in M_1$, $g \in \mathcal{F}_M$ に対して

$$
\begin{aligned}
& m_1 \geq_{M_1} \alpha_1(\gamma_1(m_1)) && ((L_1,\alpha_1,\gamma_1,M_1) \text{ is Galois connection}) \\
\implies\ & g(m_1) \geq_{M_2} g(\alpha_1(\gamma_1(m_1))) && \text{(Monotonicity of } g) \\
& \geq_{M_2} \alpha_2(\gamma_2(g(\alpha_1(\gamma_1(m_1))))) && ((L_2,\alpha_2,\gamma_2,M_2) \text{ is Galois connection})
\end{aligned}
$$

となり $\forall g \in \mathcal{F}_M, \alpha(\gamma(g)) \leq_{\mathcal{F}_M} g$.
したがって $(\mathcal{F}_L, \alpha, \gamma, \mathcal{F}_M)$ は Galois 接続.