抽象代数の基礎の復習
（半群・モノイド・群・環・体）

Akihiko Koga

Ver. 0.92 ... 2021.9.9

（Ver. 0.90 ... 2021.9.7 作成）

注意） 本資料はの使用は，個人的な勉強のためだけに留めてください．特に再配布は禁止します．

本資料について

- この資料は，別の勉強会**「ゼロによる除算の調査 Wheels, Meadows など」**の事前勉強会のための資料である
- 「ゼロによる除算～」の勉強会では，**基本的な範囲**だが，「環」，「体」などの**抽象代数の言葉**がかなりの頻度で出てくる
- 本資料はそこに登場する抽象代数の諸概念を大急ぎで追っていって，「ゼロによる除算～」の勉強会での理解を助けることが目的である
- あまりこちらの準備的な勉強会に時間を取ることはできないので，ここでは，**基本的な概念の定義や諸性質について読み合わせる程度**のことを行う
- こちらの勉強会に参加しない方も，**自分の知識の確認**や**思い出**しのために一通り目を通しておくと良いと思う

- **本資料は個人の勉強のためだけに使用し，特に，再配布はしないようにして欲しい**

(C) 2021, Akihiko Koga

内容

- **準備**
  - 集合論の言葉，λ 記法，記法についてのその他の注意
- **代数系 （A, F）**
  - 代数，部分代数，直積，準同型，同型，直積
- **1つの二項演算が定義された代数構造 (S, ・)**
  - マグマ，半群，モノイド，群
  - 半群とモノイドについての補足
- **2つの二項演算が定義された代数構造 （R, +, ・）**
  - 半環，環，整域，体
  - 商体，全商環
- **いろいろなトピックス**
  - 自由あるいは始対象，完全性定理というもの，バーコフのHSP定理
- **参考文献**

準備

集合論の言葉

- 現代数学なので**集合論**は使うが**素朴な集合論**が大まかに分かれば良い
- 「すべての集合の集まり」や「すべての可換群の集まり」など，集合と扱えないような大きな集まりは，**「クラス」**と呼ぶが，読む側は，これはあまり神経質にならずに「集合」と変換して読んでもらって構わない
- 記号は，$\in$, $\subseteq$, $\cup$, $\cap$, …など普通に使うものを想定してもらえば良い．**集合の差分**は $A \setminus B$ が主流であるが，私は記号を出しにくいのと気分が出ないので **$A-B$** を使う

- 関数については次の用語を使うので思い出しておいて欲しい
  - 関数 **$f : X \to Y$** が
    - **1:1 関数（injection）**である，あるいは，**単射**であるとは
      - $x \neq y$ ならば $f(x) \neq f(y)$ $\forall x, y \in X$ が成り立つことである
    - **上への関数（onto, surjection）**である，あるいは，**全射**であるとは
      - $\forall y \in Y$ $\exists x \in X$ $y = f(x)$ となることである．
    - **1:1かつ上への関数（bijection）**であるとは，1:1関数であり，かつ，上への関数であることである．**全単射**ともいう．

（集合の言葉，続き）

- 集合 S の**基数**（**cardinality**，大まかには要素の数）は，|S| で表す．すべての自然数の集合 **N** の基数 |**N**| は $\aleph_0$ と記す．基数が $\aleph_0$ の集合は**可算集合**という．それより大きい集合は**非可算集合**という．
- 集合 S のすべての部分集合の集合（**冪集合**，**powerset**）は 2^S あるいは $\mathcal{P}(S)$ で記す．$|S| < |2^S|$ であることを思い出しておいて欲しい．

- 集合 A, B に対して，$R \subseteq A \times B$ をAとBの**関係**という．A=B の時は，A の上の**（二項）関係**という．$(x, y) \in R$ のことを **x R y** と書くこともある．R が次の3つの条件を満たす時，R を**同値関係**という．右側には x R y の記法で書いておく
  - $(x, x) \in R$　　x R x
  - $(x, y) \in R$ ならば $(y, x) \in R$　　x R y ならば y R x
  - $(x, y) \in R$, $(y, z) \in R$ ならば $(x, z) \in R$　　x R y かつ y R z ならば x R z

- R が Aの上の同値関係のとき，Aの元を，お互い R の関係になるもの同士をまとめた集合を**A/R** と書く．$x \in A$ とRの関係にある元を集めたものを **[x]** と書く．[x] は x の**同値類**あるいは**類**と呼ばれる

λ記法

- この資料では，式が関数であることを明示するためにλ計算の記法を使うことがある
- 数学のテキストなどで，f(x) と書いたとき，この意味としてはしばしば次の2つの場合がある
  - x を受け取って，**f(x) を返す関数**
  - 値 x に対して計算された **f(x) という値**
- 通常，文脈により読み分けるが，紛らわしい場合もあるので，関数であることを明示したい場合は，λ計算の記法を使って次のように記述することにする

  λx.f(x)
- また，x の定義域を明示したいときは次のように書くこともある

  λx : Type.式　あるいは　**λx∈S.式**
- 例
  - λx.(2･x+1)
  - λn : **N**. $n^2 + 1$　　自然数上の関数

記法についてのその他の注意

- “if and only if” の略として iff を使う. これは必要十分条件，あるいは，同値の意味である.
  - 例:
    - x, y ∈ R に対して，x∼y iff x-y∈J で定義する
    - これは，日本語の言い回しに置き換えると
      x∼y が成立するのは，x-y∈J であるとき，かつ，その時に限り成立する
      という表現になる
- これも定義に関するものであるが「:=」で定義を表すことにする
  - 例: つぎの表現は A×B を := の右側の式で定義している
    - A×B := {(a, b) | a∈A, b∈B}

代数 $A = (S, F)$

代数 $A = (S, F)$

- **代数（algebra）**とは（0個の以上の）演算（関数）の集合 F が定義された集合 S のことである.
  - S ：（集合 S をこの代数の**台**または**台集合**と呼ぶことがある）
  - F = $\{f_0, f_1, f_2, \ldots\}$ ： 演算（関数）の集合
    - f_i は一般的には $S^n \rightarrow S$ の形をしている. n = 0, 1, ...
    - n を f_i の**アリティ（arity）**と言う. 各 f_i には，アリティが決まっているものとする. 一般に代数という場合はアリティは有限のものを扱う
    - このように規定された代数は A = (S, F) あるいは A = $(S, f_0, f_1, f_2, \ldots)$ のように表す
    - Fを各演算のアリティも含めて，この代数の**シグニチャ（signature）** と呼ぶ. プログラミングで考えれば，シグニチャはその代数が表す**データ型の上に定義された基本的な関数の宣言の集まり**である.
    - ここでは１つの代数，つまり，型しか扱っていないが，複数の型（many-sored）を扱うように拡張することもでき，その場合は完全に抽象データ型の関数の宣言の集合である

（つづき）

- アリティが 1 のとき，**単項演算**，2 のとき**二項演算**ということがある．

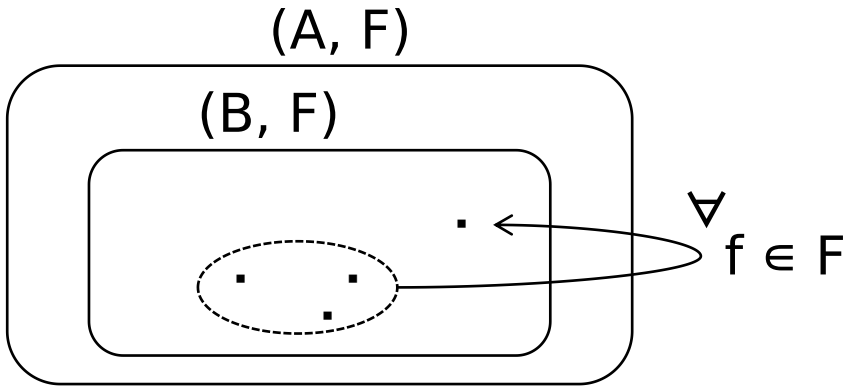
- 我々が良く使う二項演算としては，＋ や ＊ があり，関数の記法でなく，中置記法で，s_1+s_2 や s_1*s_2 のように書くことがある．このとき，＋ や ＊ を**演算子**と呼ぶことがある

部分代数

- A=(A, F) を代数とする

  この資料では，このように，代数とその代数の台集合を同じ記号で書くことがある．一般の書籍などでは，字体を変えるなどで区別するが，ここでは労力削減のために同じ字体を使うことにする．あまりに混乱が生じる場合は，字体を変えることもある．

- **定義 部分代数**
  - B⊆A が，A の**部分代数(subalgebra)**であるとは，B が F の演算で閉じていることとする．つまり
    - $\forall f \in F, \forall x_0, \ldots, x_{n-1} \in B, f(x_0, \ldots, x_{n-1}) \in B$



A の部分集合 B が∀f∈ F で閉じているとき，(B, F) は (A, F) の**部分代数**という

直積

- $\boldsymbol{A}$ = (A, F) と $\boldsymbol{B}$ = (B, F) を同じシグニチャ F の代数とする

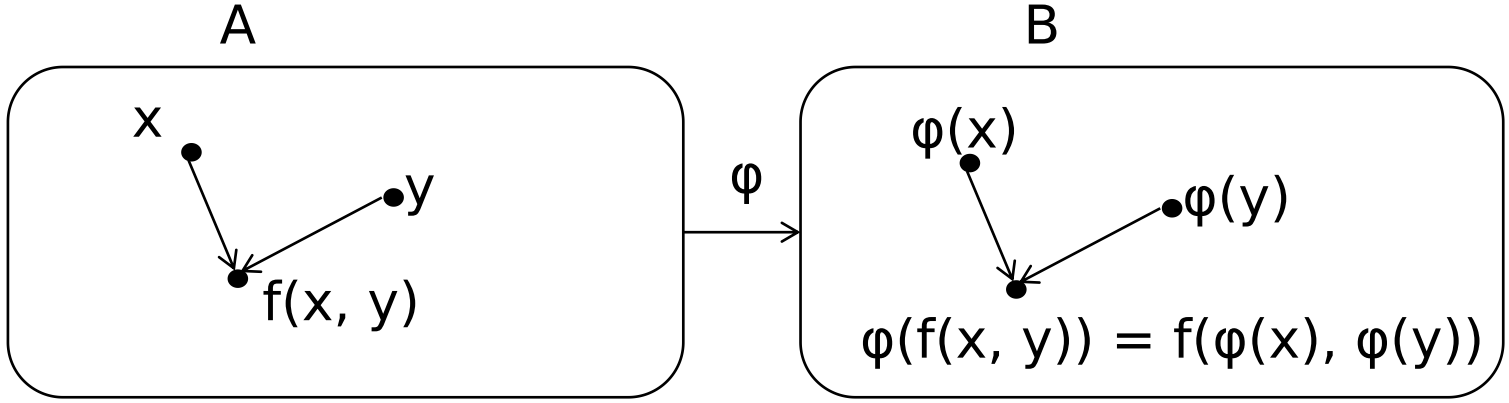
- このとき，やはり同じシグニチャの代数 $\boldsymbol{A}\times\boldsymbol{B}$ = (A×B, F) を次のように定義する.
  - f∈F に対して，**$f(\ldots, (a_i, b_i), \ldots) := (f(\ldots, a_i, \ldots), f(\ldots, b_i, \ldots))$**
  - f はそのアリティをnとするとき，$(A\times B)^n \rightarrow (A\times B)$ の関数になる

- $\boldsymbol{A}\times\boldsymbol{B}$ を代数 $\boldsymbol{A}$ と代数 $\boldsymbol{B}$ の**直積（direct prduct）**，あるいは，**積（product）**という.

準同型と同型

- **定義 準同型写像と同型**
  - (A, F) と (B, F) が同じシグニチャの二つの代数とする
  - 写像 ϕ:A→B が**準同型写像 (homomorphism)** であるというのは，次が成立することとする

$$\varphi(f(x_0, \ldots, x_{n-1})) = f(\varphi(x_0), \ldots, \varphi(x_{n-1}))$$



f が二項演算の場合の図

  - (S_1, F) と (S_2, F) が**同型**であるというのは，二つの準同型写像 ϕ_1:S_1→S_2 と ϕ_2:S_2→S_1 があり，$\phi_2 \cdot \phi_1 = id_A$, かつ，$\phi_1 \cdot \phi_2 = id_B$ となることである．ここで，id_S は，S→S の恒等写像であるとする．ϕ_1 と ϕ_2 は**同型写像**と呼ばれる．一般に，全単射の準同型写像が同型になることが多いが，必ずしもそうとは限らない．

まとめ

- A=(A, F) を**代数**という

  ただし，A は何らかの元の集合（**台集合**），F={f, g, …} は $A^n \to A$ の関数．nは各 f∈F ごとに決まっていて，f の**アリティ**という．F を各関数のアリティも含めて，**シグニチャ**という

- B⊆A に対して Bが∀f∈Fで閉じているとき，***B***=(B, F) を ***A***=(A, F)の**部分代数**という

- ***A***=(A, F) と ***B***=(B, F) を同じシグニチャ F の代数とするとき，**代数の直積** ***A***×***B***=(A×B, F) とは，各 f∈F に対してその (A×B) の上の値を次のように定義したものである．

  $\mathbf{f(\ldots, (a_i, b_i), \ldots) := (f(\ldots, a_i, \ldots), f(\ldots, b_i, \ldots))}$

- ***A***=(A, F) と ***B***=(B, F) を同じシグニチャ F の代数とするとき，関数 φ：A→B が**準同型**であるとは次の式が成り立つことであるとする．

  $\varphi(f(x_0, \ldots, x_{n-1})) = f(\varphi(x_0), \ldots, \varphi(x_{n-1}))$

- 代数 A から B への準同型写像φ_1：A→B とBからAへの準同型写像 φ_2：B→A があり，$\varphi_2 \cdot \varphi_1 = id_A$, $\varphi_1 \cdot \varphi_2 = id_B$ を満たす時，A と B は**同型**であるといい，φ_1 と φ_2 は**同型写像**という．ここで，id_A と id_B はそれぞれ，AとBの上の恒等写像を表す．

この資料で扱う代数構造

- 以下，この資料では代数 A=(A, F) の良く整理されたものを見ていく．F に含まれる関数（演算）の個数ごとにまとめると次のようなものを扱う．

  - １つの二項演算が定義された代数構造 (S, ・)
    - マグマ
    - 半群
    - モノイド
    - 群

  - ２つの二項演算が定義された代数構造 (S, +, ・)
    - 半環
    - 環
    - 整域
    - 体

一つの二項演算が定義された代数構造

$(A, \cdot)$

1つの二項演算を持った主な代数系

- ここでは次の表の代数系(A, ・)を見ていく

名称	条件
マグマ(magma)	–
半群(semigroup)	**結合法則: (x・y)・z = x・(y・z)**
モノイド(monoid)	結合法則: (x・y)・z = x・(y・z) **単位元の存在 ∃ 1 such that 1・x = x・1 = x**
群(group)	結合法則: (x・y)・z = x・(y・z) 単位元の存在 ∃ 1 such that 1・x = x・1 = x **逆元の存在 x^{-1}・x = x・x^{-1} = 1**

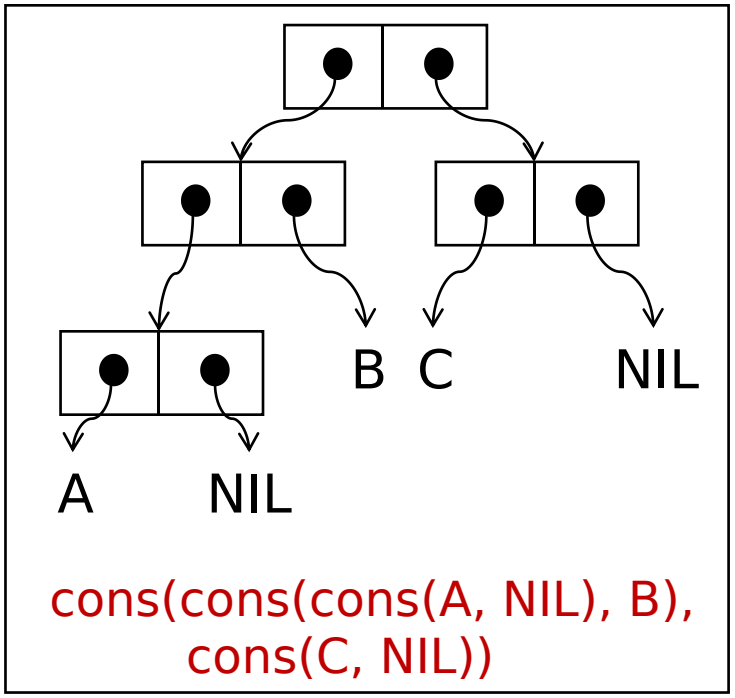
- x・y = y・x が成立するときは,**「可換(commutative)」**を代数の名称の前に付けて呼ぶ

(C) 2021, Akihiko Koga

1つの二項演算の代数系
マグマ

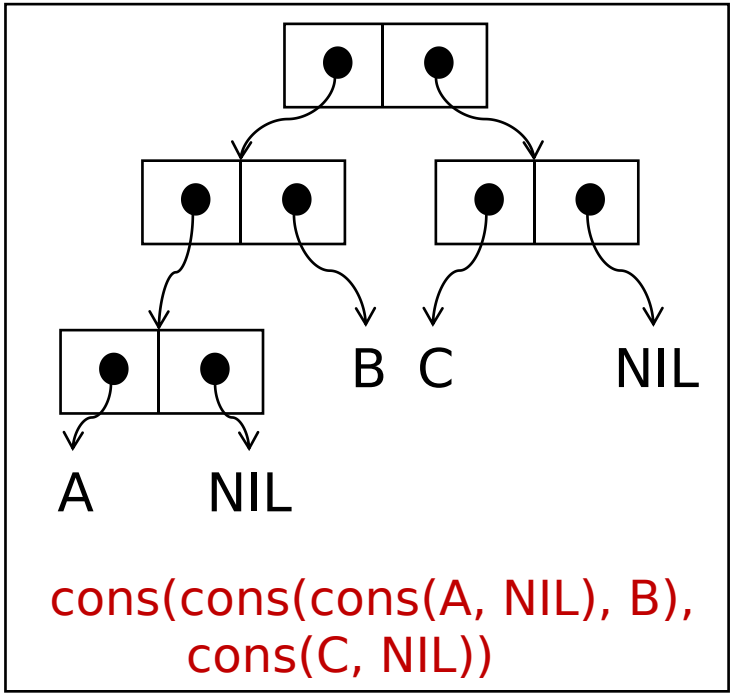
- 何か二項演算が定義された集合 A = (A, ・) が**マグマ(magma)**である
- マグマは，昔は groupoid と呼ばれていたが，結合法則や単位元の存在が保証されないなど，群(group)と成立条件に距離があるためか，この用語がつけられた
- 例
  - やや特殊かもしれないが，計算機屋さんに馴染みの例は，LISP の S-式の集合 **(S-式, cons)** である．要は2分木である．
    - **cons : S-式 × S-式 → S-式**
    - **S-式 ::= アトム | cons(S-式, S-式)**
  - LISP の すべてのS-式は究極的には，アトムに有限回の cons を適用して作られている．
  - この場合のアトムのように，その代数のすべての元を生成する元の集合を**生成元**と呼ぶ
  - LISP の場合，アトムは無限にあるので，これによって生成された代数は**無限生成**の代数という

(次頁に続く)



（続き）

- 生成元を例えば，0, 1 だけに限ることもできる．（右の図で，A, B, C, NIL は 0 か 1 かになる）
- この場合，この代数は**有限生成**であるという．
- 一般に，有限生成と無限生成では，代数の性質に違いがでることがある（例えば，「有限生成のアーベル群は巡回群の直積に分解できる」など）．



- LISP の S−式の場合，代数の要素に関する**変換規則**（例えば，cons(cons(K, x), y) は x に簡約して良いなど）は**まったくない**．このように全く要素間に変換規則の無い代数を**自由代数**と呼ぶ．実は自由代数は，規則を入れることにより，考察対象の任意の代数を作ることができる代数で非常に重要な代数である．
- まとめると，LISP の S−式の集合は代数としては，**無限生成の自由マグマ**である

（ごめん，まだ続く）

（続き）

- 自由マグマである S-式の集合にいくつかの**変換規則を等式の集合として入れた例**を1つだけ紹介しておく
- いちいち，cons を書くのは面倒なので **cons(A, B)** を **[A, B]** と書くことにする．
- 次の等式が入ったマグマは任意の**再帰関数の計算を模擬できる代数**になる

  - [**I**, x] = x　　これはあっても無くても良い
  - [[**K**, x], y] = x
  - [[[**S**, x], y], z] = [[x, z], [y, z]]

    上の式で x, y, z は任意の S-式とする．従って，等式は3つだけに見えるが，本当は無数にある

要は，SKI のコンビネータのお話である

(C) 2021, Akihiko Koga

1つの二項演算の代数系
半群とモノイド

- **半群（semigroup）**とはマグマであって，次の結合法則が成り立つものを言う
  - $(x \cdot y) \cdot z = x \cdot (y \cdot z)$　　結合法則（associatibity）
- **モノイド（monoid）**とは半群であって，次のような**単位元（identity）**と呼ばれる要素 1 が存在するものを言う
  - $1 \cdot x = x \cdot 1 = x$　　単位元（identity）の存在
    （単位元は一意に決まる）
- 例
  - 計算機屋さんに馴染みのある例として，**Σをアルファベット**（記号の有限集合）としたとき，語の連結演算を代数の二項演算として，Σ^+ が半群になり，Σ^* はモノイドになる．これらは共に**自由半群**，**自由モノイド**である．
    - Σ^+：1個以上のアルファベット内の記号の列の集合
    - Σ^*：0個以上のアルファベット内の記号の列の集合
  - $\mathbf{N} := \{0, 1, 2, \ldots\}$ とするとき，$(\mathbf{N}, +)$，$(\mathbf{N}, \cdot)$ もモノイドである
  - $\mathbf{N}^+ := \{1, 2, \ldots\}$ とするとき，$(\mathbf{N}^+, +)$ は半群であり，モノイドにはならない
- 半群とモノイドについては説明することが沢山あるので，残りは群の後に説明する

(C) 2021, Akihiko Koga

1つの二項演算の代数系
群

- 代数 (G, ・) が**群（group）**であるとは，それがモノイドであって，さらに次の公理が成り立つことである
  - $\forall x \in G,\ \exists x^{-1} \in G\ \ x^{-1} \cdot x = x \cdot x^{-1} = 1$
- 逆元は一意に決まる
- すでに言及したが，x・y = y・x が成立するときは**可換群（commutative group）**という
- 例
  - **Z** を整数の集合とするとき (Z, +) は可換群になる
  - **Q** を有理数の集合とするとき，(Q, +), (Q−{0}, ・) は可換群になる
  - **R** を実数の集合とするとき，(R, +), (R−{0}, ・) は可換群になる
  - n を正の整数とするとき，**Z**/n**Z** （**Z**/2**Z**, **Z**/6**Z** など）を次のような代数として定義する．これらは可換群になる．
    - 台集合： {0, ..., n-1}
    - 演算 ： x + y := (x + y) mod n
      （左側の + は群の演算で，右側のは整数の可算を表す）

半群とモノイドについての追加説明
半群のモノイドの重要性と推薦教科書

- 勉強会「ゼロによる除算の調査 Wheels, Meadows など」では，ゼロで割る代数体系のことを扱うので，**「ゼロ元」**などの概念についてきちんと把握しておく必要がある
- これらの概念は**半群やモノイドの上に定義され得る概念**である．したがって，ここでしばらく半群/モノイドについての基礎知識を確認しておくことにする．
- 日本における**半群/モノイドの扱い**は，群に至る**刹那の踏み台**的なところがあり，このテーマの成書は2021年現在，皆無と言って良い状況である．実は世界的にも状況は似たり寄ったりではあるが，かなり立派な成書もいくつかは書かれている
- **計算機械（オートマトン，チューリングマシンなど）は，半群として扱うこともでき**，計算機科学の人間としてはある程度の半群論は身につけておく必要がある
- 次の教科書は**コンパクト**だが，計算機科学で必要な半群論の知識を学習することができる**良い教科書**である．また，著作権も Creative Common であり，PDF を無料で入手することができる（著者名とタイトルで検索してみるとよい）

Alan J.Cain: Nine Chapters on the Semigroup Art, version 0.66.62 (2020-06-13), licenced under Creative Commons

半群とモノイドについての追加説明
基本的な諸概念

- 半群とモノイドの関係
  - S を半群とするとき，S に仮想的な単位元を付け加えることにより常にモノイドにすることができる．このモノイドは **S^1** と記されることがある

    $S^1 := S \cup \{1\}$,　$s \cdot 1 = 1 \cdot s = s$,　$1 \cdot 1 = 1$

    注意）もともと S に単位元があれば，S^1 は S のままとする
  - したがって，単位元のある無しはあまり気にすることはない．
  - これに対して，群まで拡張できる半群やモノイドはあまりない

- 半群の演算
  - A, $B \subseteq S$, $a \in S$ とする．このとき次のように定義する．
    - **AB** := $\{x \cdot y \mid x \in A, y \in B\}$
    - **aA** := $\{a \cdot x \mid x \in A\}$
    - **Aa** := $\{x \cdot a \mid x \in A\}$
    - **A^n** := $A \cdots A$　　n 個かけ合わせる

半群とモノイドについての追加説明
基本的な諸概念

- **X から生成される半群（モノイド）**
  - Sを半群とし，X⊆S とする
  - X を含む最も小さい半群を **X から生成される半群**といい **[X]** で表す
  - [X] は 1個以上の X の元の有限個の積の集合である

  - Mをモノイドとし，X⊆M とする
  - X を含む最も小さいモノイドを **X から生成されるモノイド**といい，上と同じであるが **[X]** で表す
  - [X] は 0個以上の X の元の有限個の積の集合である

半群とモノイドについての追加説明
基本的な諸概念

- 半群/モノイド (S, ·) における特徴的な元
  - **ゼロ元（zero）**
    - z·x = z for ∀x∈S が成り立つ元 z∈S を**左ゼロ（left zero）**という
    - x·z = z for ∀x∈S が成り立つ元 z∈S を**右ゼロ（right zero）**という
    - 左ゼロであり，かつ，右ゼロである元を単に**ゼロ（zero）**という
    - 半群の中で**ゼロは存在すれば一意に決まる**（z と z' がゼロなら z=z·z'= z'）
    - 左ゼロや右ゼロは複数存在し得るが，**左ゼロと右ゼロが両方存在するなら，このときもそれらは1つになる**（上の式が成り立つことに注意）

  - **ゼロ元を持ったモノイドの例**
    - S := {0, 1, 2, 3} として
      x # y := min(x + y, 3) と
      すると，3 がゼロ元になる

x # y の表

x \ y	0	1	2	3
0	0	1	2	3
1	1	2	3	3
2	2	3	3	3
3	3	3	3	3

半群とモノイドについての追加説明
基本的な諸概念

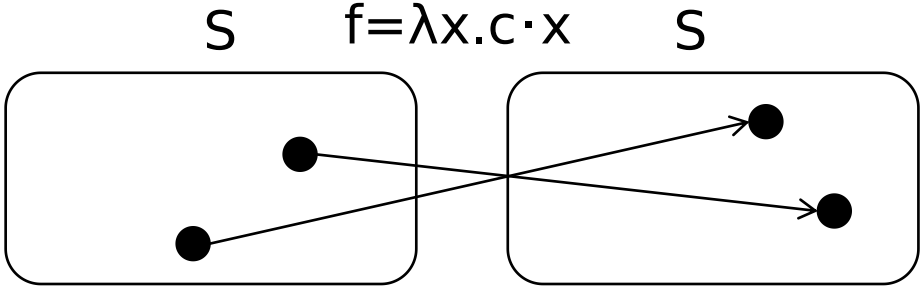
- **冪等(idenpotent)**
  - x·x = x を満たす時, x は**冪等(idenpotent)**であるという.
  - 冪等な元の典型的なものは単位元 1 である. 1·1 = 1.
  - 実際のところ, 冪等元は単位元の候補だったり, これを上手く使って単位元相当を作ったりするための重要な元である

- **unit**
  - モノイド M の元 x には逆元の存在は保証されないが, 中には逆元が存在する元もある. つまり, ある y∈M が存在して x·y = y·x = 1 となる場合である. このような x を **unit** と呼ぶ
  - モノイド M の中から, unit だけ集めた集合 G := {x∈M | x は unit} は M の演算で群をなす. これを **units の群**という.

半群とモノイドについての追加説明
基本的な諸概念

- **cancellability**
  - S を半群とする.
  - c∈S が, ∀x, y∈S c·x = c·y ⇒ x = y を満たす時, c は **left cancellable** であるという

要は関数
λx.c·x
が1:1関数(injection)であるということである



  - 同様に, ∀x, y∈S x·c = y·c ⇒ x = y であるとき, c は, **right cancellable** であるという
  - c が, left cancellable で right cancellable であるとき, 単に **cancellable** であるという.
  - S のすべての元が cancellable であるなら, S を **cancellable な半群** であるという.
  - **cancellable な半群は群に拡張できる**

半群とモノイドについての追加説明
基本的な諸概念

- **regular**
  - 半群 S の元 x が**正則（regular）**であるとは，次のような y∈S が存在することである

    $x \cdot y \cdot x = x$
  - S がモノイドで，x にたまたま逆元が存在すれば $x \cdot x^{-1} \cdot x = x$ となるので，x は regular である
  - このとき，x·y も y·x も idenpotent になる．単位元は idenpotent であることは以前に言った
  - したがって，y は逆元に近い性質をもった元である．このような y は存在するとしても，唯一に決まるとは限らない．
  - Sのすべての元が regular であるなら，S は **regular semigroup** であるという

  - 勉強会「ゼロによる除算の調査 Wheels, Meadows など」で出てくる Meadow では，逆元の公理 $x \cdot x^{-1} = 1$ を諦めて $x \cdot x^{-1} \cdot x = x$ を導入している

半群とモノイドについての追加説明
基本的な諸概念

イデアル（ideal）

- S を半群とする
- $J \subseteq S, J \neq \emptyset$ が **left ideal** であるとは $SJ \subseteq J$ となることである
- $J \subseteq S, J \neq \emptyset$ が **right ideal** であるとは $JS \subseteq J$ となることである
- $J \subseteq S, J \neq \emptyset$ が **ideal** であるとは J が left ideal であり，かつ，right ideal であることである．即ち，$SJ \cup JS \subseteq J$ となる

- ideal は環で定義されることが多いが，半群でも定義できる．基本的には 0 のように振る舞う部分集合である

principal ideal

- S を半群とし，$x \in S$ とし，S の部分集合を次のように定義する
  - **L(x)** := $S^1x = \{x\} \cup Sx$
  - **R(x)** := $xS^1 = \{x\} \cup xS$
  - **J(x)** := $S^1xS^1 = \{x\} \cup xS \cup Sx \cup xSx$

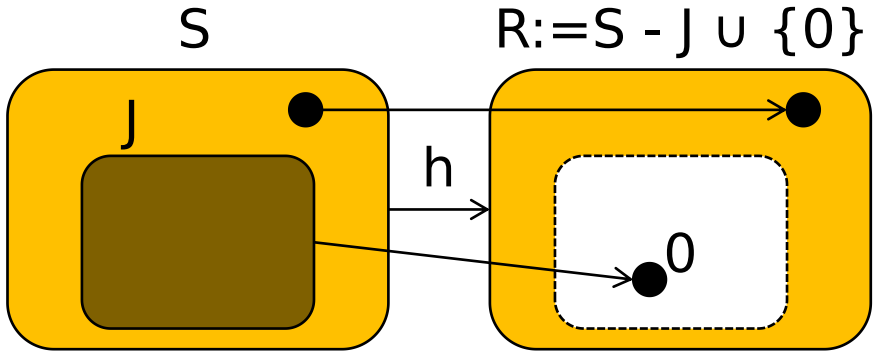
これらはそれぞれ，left ideal, right ideal, ideal である．これらを x により生成された principal left ideal, principal right ideal, principal ideal という

半群とモノイドについての追加説明
基本的な諸概念

- **Rees factor semigroup**
  - S を半群とし, J⊆S を ideal とする
  - 0 を S に含まれない元とし,

    R := S - J ∪ {0}

    の上に演算·を次のように定義する.



$$x \cdot y := \begin{cases} x \cdot y & \text{if } x, y \in S-J \\ 0 & \text{otherwise} \end{cases}$$

左の·は R の演算, 右の·はSの演算

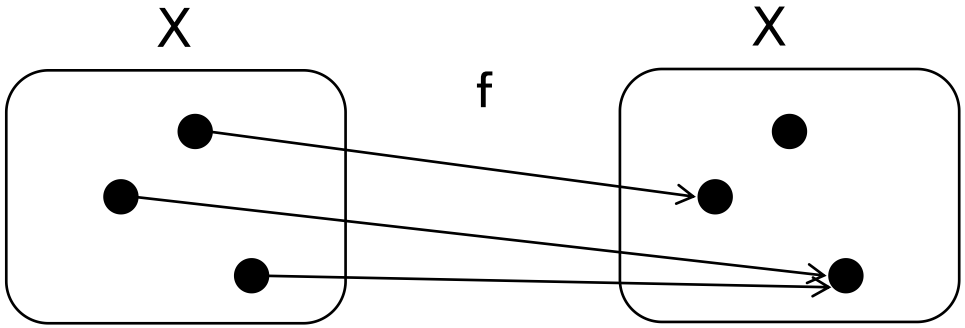
  - (R, ·) は半群になる. これを **Rees factor semigroup** という.
  - また, h : S → R h(x) = 0 if x∈J, x otherwise は準同型になる

  - これが, ideal は「0 のように振る舞う部分集合」と言った理由である
  - ideal は必ず, 何か準同型の 0 の逆像になっている

(C) 2021, Akihiko Koga

半群と群についての追加説明
重要な半群

- **変換半群（transformation semigroup）**
  - X を集合とするとき，X から X へすべての関数の集合 X→X は，関数の合成を積として，半群（モノイド）をなす．これを**全変換半群（full transformation semigroup）**という．



T_n はX から X へのすべての関数の集合（1：1で無くともよい）

  - 全変換半群は，|X| = n のとき，T_n と書くこともある．
  - Tn の部分集合 S⊆Tn が合成について閉じているとき，S は関数の合成について半群をなす．これを**変換半群（transformation semigroup）**という．
  - 変換半群は，そのなかに恒等写像 x↦x を含んでいればモノイドをなす．これを**変換モノイド（transformation monoid）**という．Tn は実は変換モノイドである．

半群とモノイドについての追加説明
半群版の Cayley の(表現)定理

- **定理(半群版の Cayley の(表現)定理)**
  半群 S はある変換半群と同型である

■ 次のようにして S と同型の変換半群を構成すれば良い
- S に単位元がなければ 1 を追加してモノイド S^1 にする
- S を $S^1 \to S^1$ の中に埋め込む同型関数 f を次のように定義する
  - $x \in S$ に対して $f(x) := \lambda u.u \cdot x$ とする
    (λu.t(u) は u を取り, t(u) を返す関数を表す)

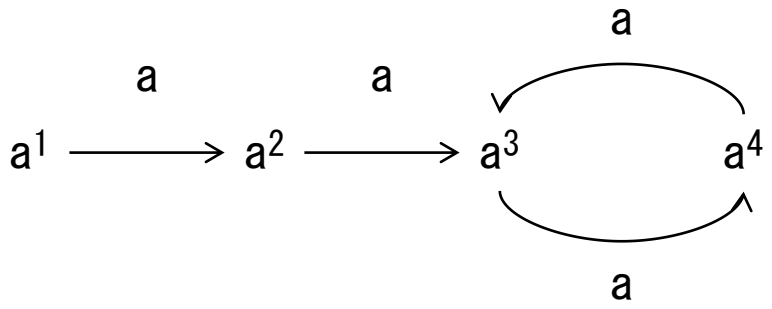
$$f(x) = \begin{pmatrix} \cdots\ u & \cdots \\ \cdots\ x \cdot u & \cdots \end{pmatrix}$$

$u \in S^1$ を $x \cdot u$ に移す.
つまり, $f(x)(u) = x \cdot u$
f(x) が $S^1 \to S^1$ の関数であることに注意

- この f により, S と $f(S) \subseteq (S^1 \to S^1)$ は同型になる.
  - $f(x \cdot y) = \lambda u.x \cdot y \cdot u = (\lambda u.x) \cdot (\lambda u.yu) = f(x) \cdot f(y)$ で準同型
  - $x \neq y$ ならば $f(x)(1) = x \neq y = f(y)(1)$ なので f は単射
  - 半群の準同型の場合, f が準同型で単射なら, S と f(S) は同型である

半群とモノイドについての追加説明
半群版の Cayley の(表現)定理

- 例:
  - a^n が次のようになる a を, ある変換半群の1つの変換として実現せよ



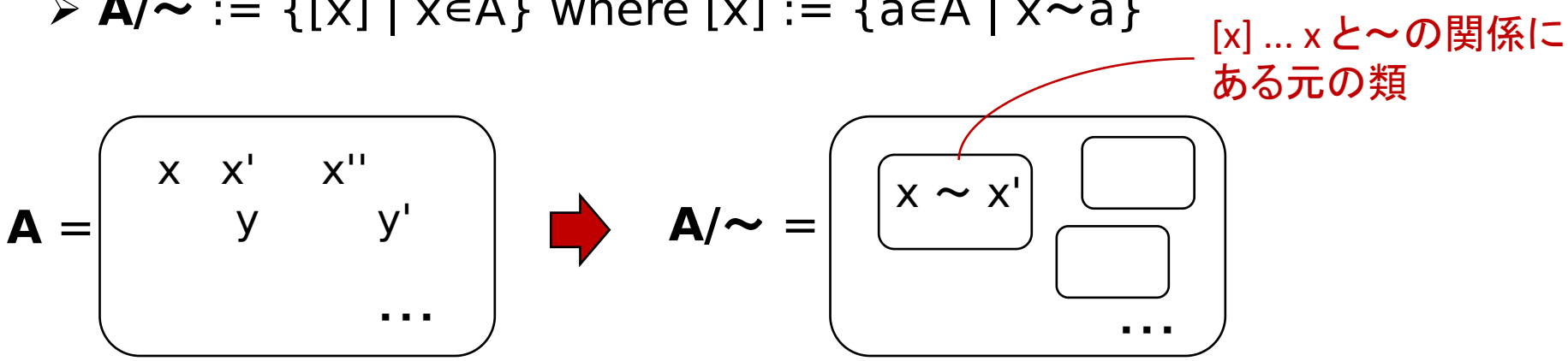
  - モノイド $M := \{1, a^1, a^2, a^3, a^4\}$ の Cayley の表現定理を使えば, a は

$$a = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 & 3 \end{pmatrix}$$

と表現される. a^n を計算すると, 上の図と同じ形になるはずである.

同値関係（equivalence）と合同関係（congruence）

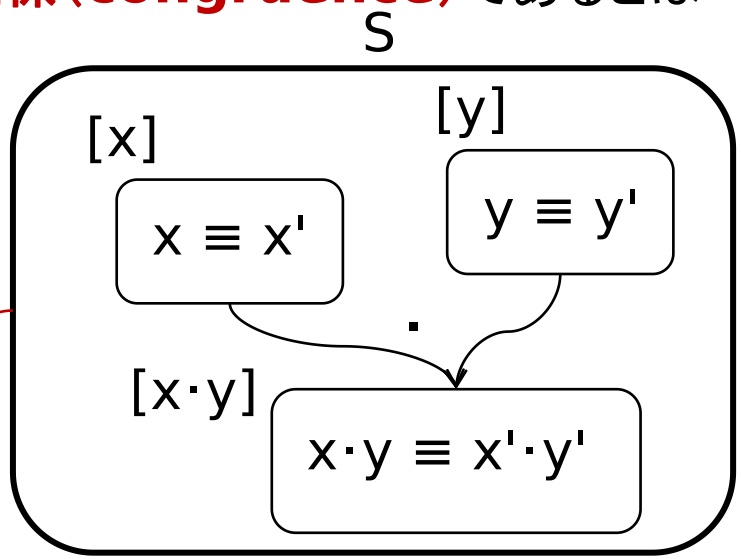
- 「集合の言葉」ですでに同値関係と同値類については説明した
  - 復習しておくと，集合 A の上に同値関係～があるとき，次のように A をお互いに～の関係にある元同士に分割した集合を考えることができるということだった
    - **A/～** := {[x] | x∈A} where [x] := {a∈A | x～a}



- 代数の場合に，このような小分けした物の代数を作るための関係が**「合同関係（congruence）」**である．合同関係は，同値関係にさらにその**代数系の演算と共立する**という要請をつける

合同関係と商代数

- 一般の代数では記号が混み入って分かりにくいので半群で説明する
- 定義
  - 半群 S = (S, ·) の上の2項関係 ≡ が**合同関係（congruence）**であるとは次の2つが成り立つことである.
    - ≡は同値関係
    - x ≡ x' かつ y ≡ y' ならば, x·y ≡ x'·y'



同じ同値類に属する元なら選び方に関わらず，演算を行った結果も同じ同値類に入る

  - このとき，S/≡ に次のように演算·を定義したものを，S の≡による商代数といい，S/≡ で表す

    [x]·[y] := [x·y]

この定義は右上の図のように well-defined である

半群の合同関係の例

- $(\mathbf{Z}, +)$ における $x \equiv y$ iff $x = y \bmod 5$
  - $x = x' \bmod 5$ かつ $y = y' \bmod 5$ ならば $x+y = x'+y' \bmod 5$ である
  - $(\mathbf{Z}, +)/\equiv$ は $\mathbf{Z}/5\mathbf{Z}$ のことである
- $J \subseteq S$ を ideal とするとき $x \equiv y$ iff $x = y \vee (x \in J \wedge y \in J)$
  - このとき $S/\equiv$ は Rees factor semigroup である
- $\varphi : (S, \cdot) \to (T, \cdot)$ が準同型のとき $x \equiv y$ iff $\varphi(x)=\varphi(y)$
  - $\varphi(x)=\varphi(x') \wedge \varphi(y)=\varphi(y')$ なら $\varphi(x \cdot y)=\varphi(x)\cdot\varphi(y)=\varphi(x')\cdot\varphi(y')=\varphi(x'\cdot y')$
  - この場合は $(S, \cdot)/\equiv$ は$(T, \cdot)$ の部分代数である $(\varphi(S), \cdot)$ と同型である
- 最後の例は，**合同関係が準同型と本質的に同等**であるということを言っている．
  - **準同型φ**があれば，**合同関係 $x \equiv y$** iff $\varphi(x)=\varphi(y)$ が作れる
  - **合同関係$\equiv$**があれば，**準同型φ** : $S \to S/\equiv$ が作れる
  - 準同型 φ に対して合同関係 $\{(x, y) \in S \times S \mid \varphi(x)=\varphi(y)\}$ をφの**核（kernel）**という

参考： 群に近い半群の例 Inverse semigroups

- 半群論でも，群に近いものについては解析が進んでいる．そのようなものの中に inverse semigroup というものがある．
- 定義
  - (S, ・) が **inverse semigroup** であるとは，1項演算 x^{-1} が定義されていて，次の式を満たすものを言う
    1. $(x^{-1})^{-1} = x$
    2. $(x \cdot y)^{-1} = y^{-1} \cdot x^{-1}$
    3. $x \cdot x^{-1} \cdot x = x$
    4. $x \cdot x^{-1} \cdot y \cdot y^{-1} = y \cdot y^{-1} \cdot x \cdot x^{-1}$

- 定理
  - S が inverse semigroup であるとする．このとき次のことが成り立つ．

    S は群である　⇔　S にはただ一つだけ idempotent がある．

(C) 2021, Akihiko Koga

２つの二項演算が定義された代数構造

$(R, +, \cdot)$

2つの二項演算を持った主な代数系

- ここでは次の表の代数系を見ていく
- 同じ集合上に定義されている二つの2項演算を + と · とし，+ を加法，·を乗法と呼ぶことにする

	加法	乗法	加法と乗法の関係	その他の条件
半環（semiring）	可換半群	半群	分配法則が成立 $x\cdot(y+z) = x\cdot y+x\cdot z$ $(y+z)\cdot x = y\cdot x+z\cdot x$	―
環（ring）	可換群	半群		―
整域（integral domain）	可換群	可換モノイド		$x\neq 0$ かつ $y\neq 0$ なら $x\cdot y\neq 0$
体（field）	可換群	0以外が群		―

- 加法は全部可換であるが，乗法も可換のものは，それぞれの名称に「可換」を付けて呼ぶ（「可換環」など）
- 整域は人によって定義が多少異なることがある（乗法の可換を仮定しないとか，乗法の単位元を仮定しないとか）．ここでは上の通りとする．

半環（semiring）

- 定義

  二つの演算が定義された代数 R=(R, +, ・) が半環（semiring）であるとは次の性質が満たされることである

  - (R, +) が可換半群であること. + は加法と呼ぶ
  - (R, ・) が半群であること. ・は乗法と呼ぶ.
    - これをモノイドとする定義もある
  - 乗法は加法の上に分配的であること
    - a・(b + c) = a・b + a・c
    - (b + c)・a = b・a + c・a

- 例
  - 1以上の自然数の集合 **N** に通常の + と ・ を定義したもの (**N**, +, ・)
    - 1 以上なので，足し算については単位元が無いことに注意
  - ブール代数 **B** = (B, ∨, ∧, 0, 1, ¬)
  - 正則言語のクリーネ代数 **K** = (K, 0, 1, +, ・, ∗) の (K, 0, 1, +, ・) の部分

環（ring）

- 代数 R=(R, +, ·) が**環（ring）**であるとは，R が半環であり，かつ，加法 + が可換群になることである．具体的に書き下すと次のようになる．
  - (R, +, 0) が**可換群であること**．+ は**加法**と呼ぶ．
  - (R, ·) が**半群であること**．·は**乗法**と呼ぶ．
  - **乗法は加法の上に分配的**であること
    - **a·(b + c) = a·b + a·c**
    - **(b + c)·a = b·a + c·a**
  - 乗法が可換である時，R は**可換環**であるという
  - また，乗法の単位元 1 があるとき，単位元のある環，あるいは**単位的環**という．

（つづき）

- 例
  - $(\mathbf{Z}, +, \cdot)$ は環である．この環は可換環であり，単位的環でもある
  - $(\mathbf{Z}/4\mathbf{Z}, +, \cdot)$ は可換環である
    - $\mathbf{Z}/4\mathbf{Z} = \{0, 1, 2, 3\}$
      - $x + y := (x + y) \bmod 4$
      - $x \cdot y := (x \cdot y) \bmod 4$

左側の + と · は，この環の演算．
右側のものは通常の整数の演算．

- 乗法の演算表は次のようになる．

$x \cdot y$ の演算表

x \ y	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

- 0 は乗法に関してゼロ元である（掛け算の結果が自分自身になる）
- $2 \cdot 2 = 0$ であり，0 以外のものを掛けて 0 になることがある．

（続き）

その他，環の例としては次のようなものがある

- 係数をある環 R に持つ**多変数の多項式全体の集合 $R[x_1, x_2, \ldots, x_n]$** は環である
- Rを環とする．このとき R から R への**関数全体の集合 $(R \to R)$** は次の演算の定義で環になる
  - f, g∈(R→R) に対して
    - f + g := λx.(f(x) + g(x))
    - f·g := λx.(f(x)·g(x))
- S を集合とするとき，**$(2^S, +, \cdot)$** は環になる
  - X + Y := (X ∪ Y) - (X ∩ Y)
  - X·Y := X ∩ Y

（その他，行列の環など例は多数）

（続き）

- 環の用語をいくつか説明しておく

  - **ゼロ因子（zero divisor）**
    - 環の 0 でない元 a が，**左ゼロ因子（left zero divisor）**であるとは，$a \cdot b = 0$ となる 0 でない元 b が存在することとする．
    - 同様に，環の 0 でない元 a が**右ゼロ因子（right zero divisor）**であるとは，$b \cdot a = 0$ となる 0 でない元 b が存在することとする．
    - 左かつ右ゼロ因子である元 a は，単に**ゼロ因子（zero divisor）**であると言われる．
    - 例えば，環の例で示した **Z**/4**Z** の **2** はゼロ因子である

  - **unit**
    - 半群の時も同様の概念を定義したが，環 R の元 x に逆元 x^{-1} が存在するとき，x を unit という．

（続き）

- **環のイデアル（ideal）**
  - R = (R, +, ·) を環とする
  - J⊆R が**イデアル（ideal）**であるとは次の条件が満たされることである
    - J は加法 + について閉じている．即ち x, y∈J ならば x+y∈J
    - RJ := {r·j | r∈R, j∈J} ⊆ J
    - JR := {j·r | r∈R, j∈J} ⊆ J

- **環 R のイデアル J による剰余環 R/J**
  - x, y ∈ R に対して，x～y iff x-y∈J とすると，これは合同関係になる
  - R/～は環になる．これを**環 R のイデアル J による剰余環**と言い **R/J** と記す
  - R/J の乗法部分に限れば，これは半群のときに説明した Rees factor semigroup である．

整域(integral domain)

- 整域(integral domain)は，整数(integer)全体のなす環を一般化した環である
- 定義
  - 乗法の単位元 1 を持つ可換環 R=(R, +, ・) が**整域(integral domain)** であるとはR がゼロ因子を持たず，かつ，自明環(|R| = 1) で無いことである.
    - つまり，x, y∈R が x≠0 かつ y≠0 なら x・y≠0 が成り立つ単位的な可換環で自明でないものである
- 例
  - 当然，整数の環 (Z, +, ・) は整域である
  - (**Z**/5**Z**, +, ・) も整域である.
  - しかし，(**Z**/4**Z**, +, ・) は，2・2= 0 になるので整域ではない

体（field）

- 0 による割り算を除いて，四則演算が自由に行える代数
- 定義
  - 整域（integral domain） F = (F, +, ·) が**体（field）**であるとは，F - {0} が乗法に関して群をなすことである.
- 例
  - 有理数の集合 **Q**
  - 実数の集合 **R**
  - 複素数の集合 **C**
  - (**Z**/5**Z**, +, ·)
    - $1^{-1}=1$ $(1\cdot 1 = 1 \bmod 5)$
    - $2^{-1}=3$ $(2\cdot 3 = 6 = 1 \bmod 5)$
    - $3^{-1}=2$ $(3\cdot 2 = 6 = 1 \bmod 5)$
    - $4^{-1}=4$ $(4\cdot 4 = 16 = 1 \bmod 5)$
  - より一般に p を素数とするとき，(**Z**/p**Z**, +, ·) は体になる

商体(field of fractions)

- **動機**
  - 体は，0 による割り算を除いて，自由に四則演算ができ，我々が計算を行う場としては，非常に優れたものである.
  - 従って，我々が考察する対象の領域を，(加法や乗法の逆元を補って)出来るだけ体に近づけることができれば有難い
  - 特に，整域は，整数の分数(fractions)を一般化した概念を使って，体にすることができる. この体は，商体というが，分数で作る体なので**分数体(field of fractions)**とも言う.
  - 勉強会「ゼロによる除算の調査 Wheels, Meadows など」で紹介する代数構造 Wheel では，このノリで，分数 Wheel(Wheel of dractions)などの代数構造を作っていく
  - ということで，この ”～ of fractions” は使い手のある言葉である

（続く）

- **商体（field of fractions） Q(R) を作る手法**
  - R = (R, +, ·) を整域とする.
  - R×(R-{0}) に次の合同関係～を導入する

    (x1, y1)～(x2, y2)　　iff　　x1·y2=x2·y1
  - この時, **Q(R)** := (R×(R-{0}))/～　は, 次の演算の定義で 体になる

    (x, y) が属する類（class）を [x, y] と書くことにする

    - 0 := [0, 1]
    - 1 := [1, 1]
    - [x1, y1] + [x2, y2] := [(x1·y2 + x2·y1), y1·y2]
    - [x1, y1] + [x2, y2] := [(x1·y1), (x2·y2)]

(C) 2021, Akihiko Koga

（続く）

- この定義は類を [x, y] の記法で書くと分かりにくいが，**[x/y]** と書くと，普通の分数の計算である
  - **0 := [0/1]**
  - **1 := [1/1]**
  - **[x1/y1] + [x2/y2] := [(x1·y2 + x2·y1)/(y1·y2)]**
  - **[x1/y1]·[x2/y2] := [(x1·x2)/(y1·y2)]**
- x≠0, y≠0 のとき，[x/y] の**逆元**は [y/x] である
  - [x/y]·[y/x] = [(x·y)/(x·y)] = [1/1] = 1

  （整域であるので，x≠0, y≠0 ならば x·y≠0 となることに注意）
- **もとの整域 R の商体への埋め込み**
  - R の元 r∈R は [r/1] に対応させることにより，商体 Q(R) は，環（整域）R を拡張した体と考えることができる．逆に言えば，r ↦ [r/1] は R を Q(R) に埋め込む写像である．

全商環(total ring of fractions)

- 動機
  - 整域は分数(fractions)を追加していくことにより，商体という体に拡張することができた
  - 整域でない一般的な環では，ゼロ因子(a≠0 かつ b≠0 だが a·b=0)があるため，体にすることはできない
    - a, b をゼロ因子とすると，

      $$[1/a]\cdot[1/b] = [1/(a\cdot b)] = [1/0]$$

      となり，計算結果の [1/0] が，R×(R-{0}) の類に収まらなくなってしまう
  - しかし，体にならなくとも，出来るだけ逆元が存在する領域というものは有難いという考えもある
  - 環から商体を作る手続きで，出来る限り乗法についての逆元を加えていくことで，体に近い環に拡張することができる．これも分数を加えていくことによる拡大なので，英語では **total ring of fractions** という．日本語では**全商環**である．

（続き）

- **全商環 Q(R) の作り方**
  - R=(R, +, ·) を単位元のある可換環とする
  - **S**⊆R を R のすべての**ゼロ因子でない元の集合**とする
  - R×S に合同関係～を次のように導入する
    - (x, s) ～ (y, t)　　iff　　x·t = y·s
  - **Q(R)** := (R×S)/～ に演算を次のように定義する．商体での説明のように，(x, s) の類を [x/s] と書くことにする
    - **0 := [0/1]**
    - **1 := [1/1]**
    - **[x/s] + [y/t]** := [(x·t + y·s)/(s·t)]
    - **[x/s]·[y/t]** := [(x·y)/(s·t)]
  - 全商環も商体と同じ Q(R) で表す
  - R の元 r は r ↦ [r/1]∈Q(R) で，Q(R) の中に埋め込まれる

（続き）

- $x \in S$ に対して，$[x/1] \cdot [1/x] = [x/x] = [1/1] = 1$ となり，逆元が存在する
- $a \cdot b = 0$ に対しては，$[1/a]$ は，a が S に属していないので，Q(R) には存在できず，逆元は存在しない
- R が整域の場合は，$S = R - \{0\}$ となるので，Q(R) は商体と一致する（つまり，Q(R) は体になる）

- **勉強会「ゼロによる除算の調査 Wheels, Meadows など」に向けて**
  - このように整域でない環からは体を作ることができないし，また，整域でも 0 の逆元を扱うことが出来なかった
  - 今度の勉強会でとりあげる代数構造 Wheel では，商体や全商環の構成を少し修正して，0 の分母の「（新しい）数」も許した代数を考える
  - ただし，残念ながら，$(3/0) \cdot 0 = 3$ のような計算ができるようになる訳ではない
  - 代数体の構成の比較のために全商体の構成方法をしっかり把握しておいて欲しい

ご参考：環上の加群（Module）

- ベクトル空間を一般化した概念である．次の定義で，R がスカラー，M がベクトルに対応する．
- 定義
  - R を環とする．(M, +) を可換群とする
  - 可換群 (M, +) が R 上の**左 R 加群（module）**であるとは，

    $\cdot : R \times M \to M$

    の作用が定められていて，次の条件を満たすことである．

    $\alpha, \beta \in R$, $1_R \in R$ は乗法の単位元, $x, y \in M$ に対して

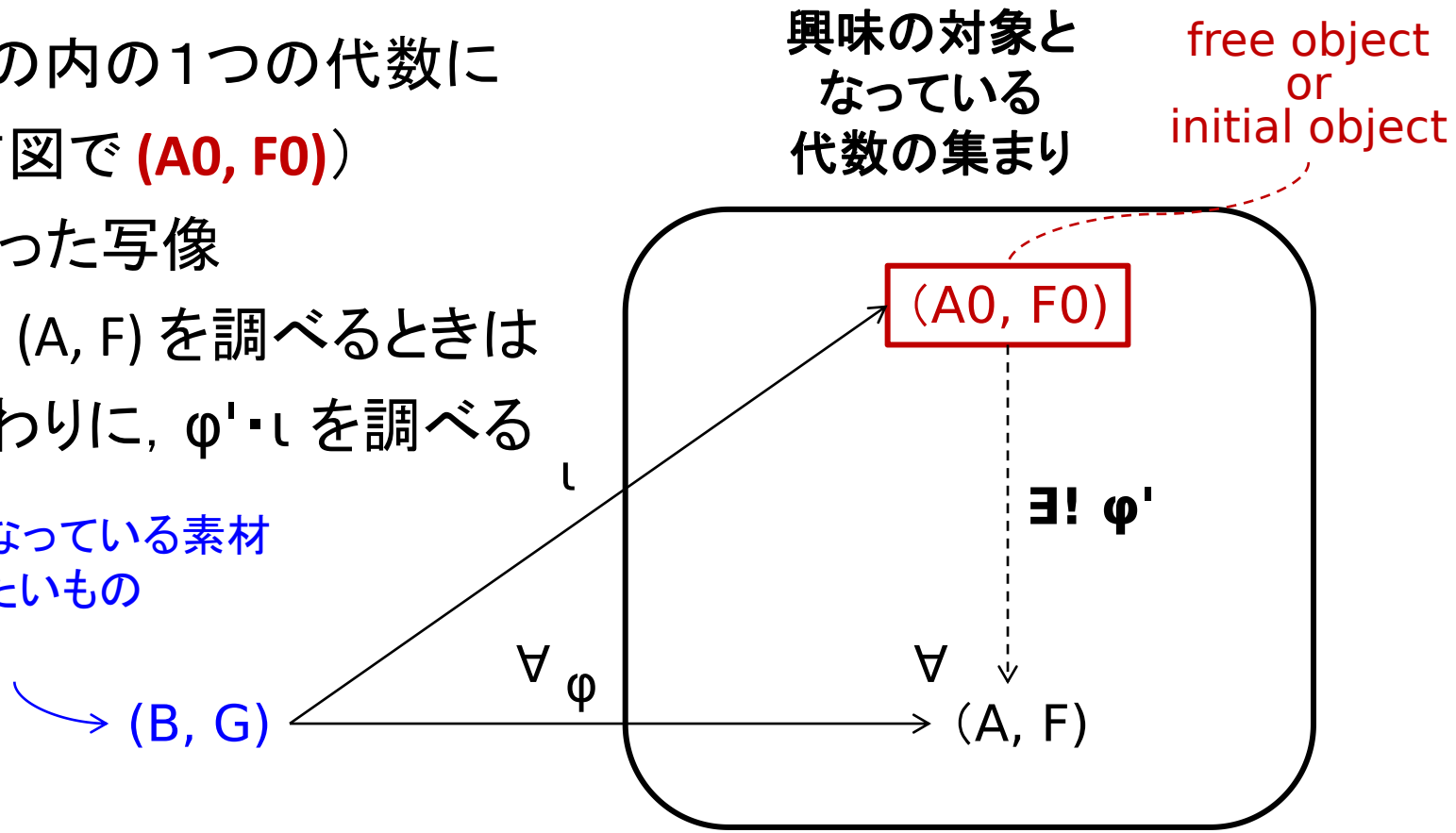
    1. $\alpha \cdot (x + y) = \alpha \cdot x + \alpha \cdot y$
    2. $(\alpha + \beta) \cdot x = \alpha \cdot x + \beta \cdot x$
    3. $(\alpha \cdot \beta) \cdot x = \alpha \cdot (\beta \cdot x)$
    4. $1_R \cdot x = x$

  - 同様に**右 R 加群**も定義される

いろいろなトピックス

自由(free)あるいは始対象(initial object)

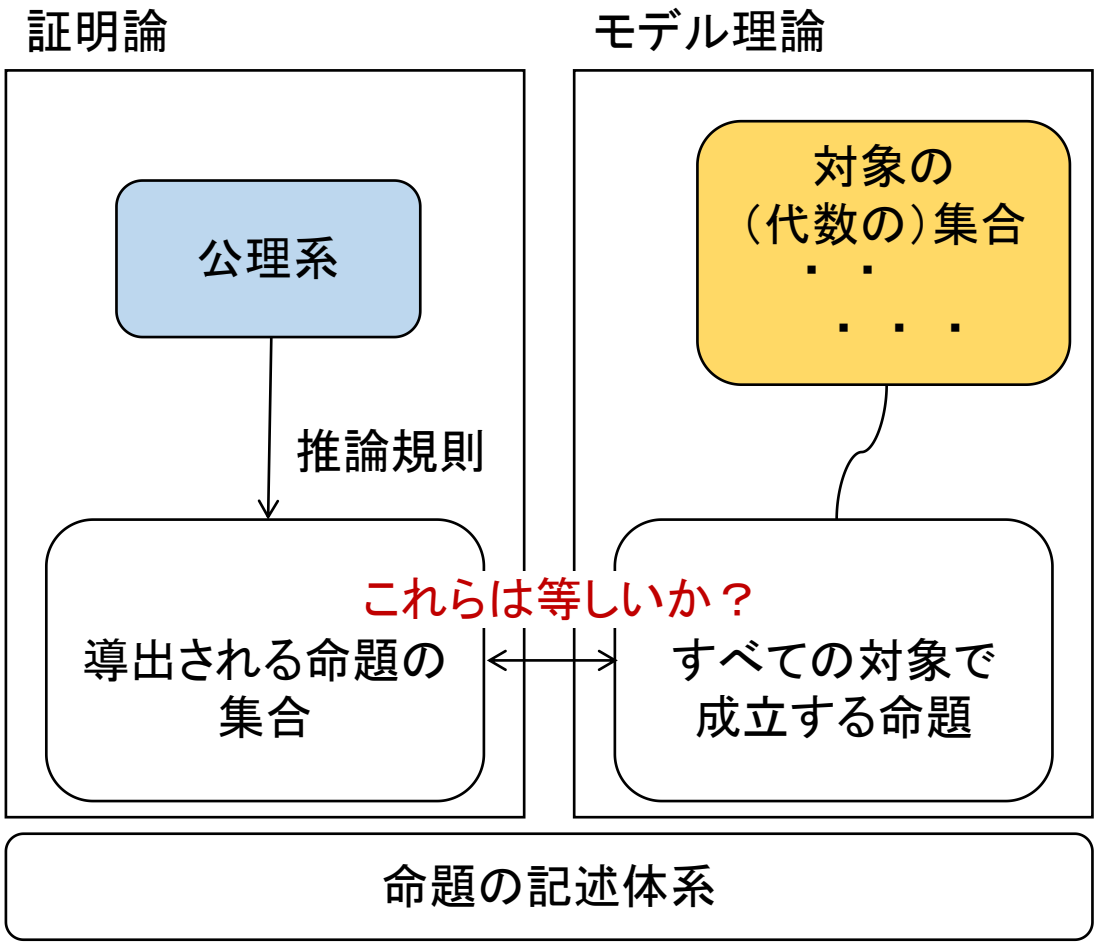
- 考察対象の代数の集まり **C** をできるだけ楽に，統一的な方法で扱いたい
- 対称の集まりの内の1つの代数に代表させる(右図で **(A0, F0)**)
- 図中 ι は決まった写像
- **C** の中の代数 (A, F) を調べるときは φ を調べる代わりに，φ'･ι を調べる



構成の元になっている素材
関係を調べたいもの
・・・

一般に「完全性定理」というもの

- 勉強会「ゼロによる除算の調査 Wheels, Meadows など」を念頭に置いて説明する
- 最初に，0 で割ることに意味のありそうな**代数の族**を何らかの方法で構成する．それが右の上の**「対象の（代数の）集合」**である
- 次にそれらの代数で共通に成り立つ性質を調べる．それらの性質の中から，対象の代数を規定できそうな**公理系の構築を試みる**
- その**公理系が妥当か**どうかの一つの基準として，最初に構築した**「対象の（代数の）集合」で共通に成り立つ性質がすべて導出できるか**という基準がある
- これが成り立つというのが**完全性定理**である



(C) 2021, Akihiko Koga

バーコフのHSP定理

- **代数のクラス Variety**
  - 代数のシグニチャ Σ と，その代数が満たすべき性質が等式の集合 Eqs が与えられているとする．
  - このとき，シグニチャ Σ を持ち，等式 Eqs を満たす代数のクラス（集まり）を **variety** という．
  - 例えば，**群のクラス**は，シグニチャ $\{1, \cdot, ^{-1}\}$ を持ち，次の等式の集合を満たす代数であるから，variety である．ここで，単位元は代数の要素であるが，$A^0 \to A$ の関数とも考えられる．等式において定数を表す枠組みがないので，定数はこのような関数として表すことにする．
    1. $(x \cdot y) \cdot = x \cdot (y \cdot z)$
    2. $1 \cdot x = x$
    3. $x \cdot 1 = x$
    4. $x \cdot x^{-1} = 1$
    5. $x^{-1} \cdot x = 1$
  - 要は**等式の集合で規定される代数のクラス**のことを **variety** という

（続き）

- **Variety の例と反例**
  - 上で**群のクラスが variety であること**を見たが，同様に，**可換群**のクラス，**半環**のクラス，**環**のクラスも variety である．
  - しかし，**体のクラスは variety ではない**．それは逆元の性質が等式だけでは表現できないからである．0 の逆元がないので，次のように条件部が必要になってしまう．

    $x \neq 0$ ならば $x \cdot x^{-1} = 1$

- **Variety の価値**
  - 代数が等式だけの公理で規定できるという性質は，項の書き換えだけで，その代数に関する性質を導出することができ，一般には**嬉しい性質**である

（続く）

- 同じシグニチャの代数のクラスが variety かどうか，すなわち，等式の集合で規定できるかどうかは，次のような簡単な特徴づけがある

- **バーコフのHSP定理（1935）**
  - Σ を代数のシグニチャとする
  - Σ のシグニチャを持つ代数のクラス **A** が variety である必要十分条件は A が，次の3つの操作で閉じていることである.
    - 準同型（**H**omomoriphism）の像を作る操作
    - 部分代数（**S**ubalgebra）を取る操作
    - 直積（**P**roduct）を取る操作

- 体のクラスは，準同型の像，部分代数，直積で閉じていない

参考文献

- 次の参考文献はインターネットで検索してもらえば PDF が見つかる

- **半群**
  - Alan J.Cain: **Nine Chapters on the Semigroup Art**, version 0.66.62 (2020-06-13), licenced under Creative Commons
    - かなり良い本である．半群論の基礎から，ちょっと発展的なトピックス（普遍代数，Variety，オートマトンなど）まで展開されている．記述は平易で，しかも重要な語は本文の左右に見出し語として書かれている．

- **群・環・体**
  - Thomas W. Judson, Stephen F. Austin State University: **Abstract Algebra: Theory and Applications**, 2016, licensed with a GNU Free Documentation License (GFDL)