代数系への入門
モノイド・群・環

松本　眞[1]

2020 年 9 月 24 日

[1]広島大学理学部数学科 m-mat@math.sci.hiroshima-u.ac.jp

目 次

はじめに

代数とは、和や積などの「元と元との演算」が行え、それらが分配法則などの「性質」を満たしているような構造である。数学のほとんどいたる分野において、自然にこのような構造が共通に見られるため、それらに慣れ親しんでおくことは見とおしの良さにつながる。数学の長い歴史を通して、重要であると見なされるようになった三種の構造である、「群、環、体」を通して、代数学の基礎を学ぶのがこの本の目的である。また、本書の特徴として、半群・モノイドというより構造が簡単な代数系を導入することにより、学修のハードルを下げる試みが図られている。半群・モノイドは、計算機科学などで近年重要性を増しているが、それを扱う代数学の書籍は少ないと感じている。

代数系は、抽象的な公理により記述される。僕自身がそうであったように、初学者は、現代数学がこのように性質＝公理により記述されているのを見てあまりにも機械的で味気ないと思うかも知れない。が、慣れてくるとこれは是非とも必要で、便利で強力な方法だとわかってくる。

具体例を挙げてみる。

$$(ab)^{-1} = a^{-1}b^{-1} \tag{1}$$

という公式を、高校生なら知っていると思う。ここで、高校では暗黙のうちに a, b は実数であると考えることにしている。そして、実は複素数でも成立する、と習う。ところが、a, b が 2×2 行列となると、一般には成り立たない。成り立つのは

$$(ab)^{-1} = b^{-1}a^{-1} \tag{2}$$

である。そして、(2) の形になると、a, b は任意の合成可能な一対一写像でも成立する。

では、(1) や (2) はどんなものに対して成立し、どんなものに対しては成立しないのか？高校までの数学では、(1) は有理数、実数、複素数では成立するが行列では成立しない、などと個別に習う。この方法だと、新しい数の体系を考えるごとに、(1) が成立するかどうか調べないとならない。

現代数学では、有理数、実数、複素数など特定の数の集合を考える代わりに、それらが共通に満たす性質であって「筋のいいもの」を列挙する。そして、「それらの性質を満たす」という仮定だけから、何が証明できるか—(1) や (2) は証明できるか—を調べておく。列挙された筋のいい性質のことを公理といい、そこから証明されたことを定理という。こうすれば、新しい数学的体系を考え出したとき、それらがどの公理を満たすか調べれば、どの定理が成り立つかわかる。

その上、公理は筋がいいものを少数選んだだけであるから、証明する際に（使える情報が少ないので却って）うまく行くかどうかがわかりやすい。たとえば、(1) が実数に対して成立するかどうかは、実数の大小などの順序構造をまったく知らなくても調べられる。

実際、(2) はモノイドの公理と呼ばれる極めて一般なたった 2 つの公理を満たす体系で証明

できる定理である（問題 2.19）。そして、有理数、実数、複素数、行列のどれもが積に関してモノイドの公理を満たしている。

読者はしかし、こう説明されても納得はできないかも知れない。この本を読んでいくうちに、あるいは何年か現代数学に慣れ親しむうちに、これらの言葉がばかばかしいほど当たり前に思えてくることと思う。

この本を書くに当たって、筆者は「自分が初めて代数を習ったときに感じた戸惑いと喜び」を思い出しつつ執筆するように留意した。群、環やその準同形などは、「なぜこんな風に定義するのか」さっぱりわからなかった。後日、さまざまな経験を積み、また普遍代数の基礎を学ぶ機会があり、この疑問に対するかなり納得の行く答を得ることができた。この本では、いろいろなものを取り入れて「納得の行く」説明をするように心がけている。そのため、通常の代数の教科書が軽く扱い勝ちである、半群やモノイドを群に先立って導入した。また、同値類と写像に関して、多くの教科書が説明をしない「集合と写像に対する準同形定理」を群や環の準同形定理に先立って解説した。

数学の血は限りなく古く、そして新しい。たとえば計算機科学など比較的新しい分野で、データ構造やデータベースの構築に際し、関係や演算や公理など、（古典的な普遍）代数の概念が有用になることがある。このような点からも、通常の教科書では無視されがちな基礎的事項—演算とは何か、同値関係とはなにか、それらがコンパチブルであるとはどういうことか、など—について、最初の方で解説しておくことにした。

第1章　集合、写像、演算

1.1　集合と写像

以下のような事項を理解している必要性がある。

1. 集合、写像
2. 全射、単射
3. 逆写像、可逆な写像
4. 全単射であることと逆写像が存在することとが同値
5. 逆行列と、逆写像の関係
6. 集合の直積

これらの事項を理解していれば、この節 1.1 は飛ばして良い。

1.1.1　集合

集合（set）とは、「ものの集まり」のことである。これ以上きちんと定義することはしない。集合に属するひとつひとつのものを、その集合の**元**または**要素** (element) という。

$$\{1, 2, 3\}$$

と書いたら、1,2,3 なる三つの元からなる集合を表す。

$$\{1, 2, 2, 3\}$$

と書いたら「1 を一個、2 を二個、3 を一個含む集合」のように見えるだろうが、このように同じ元を重複して含んでも一つの元として考える（重複の個数も考えた「ものの集まり」は**多重集合** (multi-set) と呼ばれるが、ここでは扱わない）。重複して書かれても一個の元と考える。したがって、

$$\{1, 2, 2, 3\} = \{1, 2, 3\}$$

である。$\mathbb{N}$ で自然数の集合、$\mathbb{Z}$ で整数の集合、$\mathbb{Q}$ で有理数の集合、$\mathbb{R}$ で実数の集合、$\mathbb{C}$ で複素数の集合を表す。したがって、

$$\mathbb{N} = \{1, 2, 3, \ldots\}$$

である。

$$\mathbb{Z} = \{0, 1, -1, 2, -2, \ldots\}$$

であり、

$$\mathbb{Q} = \left\{ \frac{n}{m} \mid n \in \mathbb{Z}, m \in \mathbb{N} \right\}$$

である。この最後の記法では、縦線 | のあとに書かれているものは条件を表している。すなわち、「$\frac{n}{m}$ なるものを集めなさい。ただし条件があります。n は整数で、かつ m は自然数です」という意味である。

元の数が有限個であるような集合を**有限集合**といい、無限個であるような集合を**無限集合**という。$\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ はいずれも無限集合であるが、$\{1, 2, 3\}$ は有限集合である。

集合 S に対し、S の元の個数を S の**濃度** (cardinality) といい、$\#(S)$ または $|S|$ で表す。多くの本で $|S|$ のほうが採用されているが、絶対値と紛らわしいのでここでは $\#(S)$ を使う。$\#(\{1, 2, 3\}) = 3$ であり、$\#(\mathbb{N}) = \infty$ である。

注意 1.1.1. 無限集合といってもいろいろな種類がある。$\mathbb{R}$ の元の個数は $\mathbb{N}$ の元の個数より真に大きい。前者を連続濃度、後者を可算濃度という。これについてより正確に知りたい読者は、適切な教科書 ([1] など) を参照してほしい。

集合 S の元がどれも集合 T の元であるとき、S を T の**部分集合**と言い、$S \subset T$ であらわす。

元をひとつも含まない集合を**空集合**といい、$\emptyset$ で表す。すなわち

$$\emptyset := \{\}.$$

注意 1.1.2. 上の式の中の $:=$ の意味は、「左辺を右辺により定義する」の意味である。

集合 S, T に対しその**共通部分** (intersection of S and T) を $S \cap T := \{x \mid x \in S \text{ かつ } x \in T\}$ で定義し、その**合併集合** (union of S and T) を $S \cup T := \{x \mid x \in S \text{ または } x \in T\}$ で定義する。

1.1.2　直積

定義 1.1.3. 二つの集合 S, T に対し、その**直積** $S \times T$ を、S の元と T の元の組の全体の集合と定義する。すなわち、

$$S \times T := \{(s, t) | s \in S,\ t \in T\}.$$

三つ以上の集合の場合も同様に、

$$S \times T \times U := \{(s, t, u) | s \in S, t \in T, u \in U\}$$

と定義する。$S \times S$ を S^2 と書く。n を自然数とするとき、n 個の直積 $S \times S \times \cdots \times S$ を S^n と書く。これは、「() の中に S の元を n 個並べたものの集合」である。こう考えると、S^1 は $\{(s) | s \in S\}$ となるのであるが、S と同一視するのが普通である。

S^0 はどう定義するべきであろうか？上で $n = 0$ と考えると、0 個並べるのだから答は

$$S^0 = \{()\} \tag{1.1}$$

なる 1 元集合である。

1.1.3 写像

二つの集合 S, T に対し、S から T への**写像** (mapping) とは、S の元に対して T の元をただひとつ定める定め方のことである。写像のことを**関数** (function) ともいう。その頭文字をとって、写像をしばしば f で表す。$s \in S$ に対して、f が定める T の元のことを $f(s)$ と表し、s の f による**像** (image) という。

例 1.1.4. 高校などではしばしば

$$f(x) = x^2 - 2x + 1$$

と書いて関数（＝写像）を定義する。が、これだけでは「どこからどこへの関数か」がはっきりしない。高校では、暗黙のうちに上のような $f(x)$ は「実数の集合から実数の集合への写像」だと理解していた。「実数 x をもらって、$x^2 - 2x + 1$ を計算して返す仕組み」、それを上のように書き表していたのである。

大学では、写像といったら、「どの集合からどの集合への写像なのか」をはっきりさせておかなくてはならない。

f が集合 S から集合 T への写像であることをあらわすのに、

$$f : S \to T, \quad S \xrightarrow{f} T$$

などと表す。この状況を、ひとつの図（図式、diagram という）で表して

$$\begin{array}{rccc} f: & S & \to & T \\ & s & \mapsto & f(s) \end{array}$$

のように記述する。S を f の**定義域** (domain) あるいは**始集合**、T を f の**値域** (codomain) あるいは**終集合**と言う。しっぽなしの矢印 $\to$ は、始集合と終集合を結ぶ記号であるのに対し、しっぽつきの矢印 $\mapsto$ は、「この元をこの元に写す」ということを表している。

例 1.1.5. 例 1.1.4 の関数を図式であらわせば、

$$\begin{array}{rccc} f: & \mathbb{R} & \to & \mathbb{R} \\ & x & \mapsto & x^2 - 2x + 1 \end{array}$$

となる。

注意 1.1.6. 同じ式が、複素数から複素数への写像

$$\begin{array}{rccc} f: & \mathbb{C} & \to & \mathbb{C} \\ & x & \mapsto & x^2 - 2x + 1 \end{array}$$

を定めたりもする。この f は、上の f とは始集合・終集合が異なるという点から違う写像であると考える。

定義 1.1.7. S, T を集合とする。S から T への二つの写像 f, g が等しいとは、任意の $s \in S$ に対して $f(s)$ と $g(s)$ が等しいことである。つまり、どんな s をもらっても、計算結果である $f(s)$ と $g(s)$ が等しいことである。このとき、$f = g$ と表す。

たとえば、実数の部分集合 $S = \{0, 1, 2\}$、 $T = \{0, 1\}$ を考える。S から T への関数 $f(s) = s^2 - 2s + 1$ と $g(s) = |s - 1|$ とは等しい、すなわち $f = g$。だが、同じ式で $\mathbb{R}$ から $\mathbb{R}$ への関数を定めると、$f \neq g$ である。

注意 1.1.8. 上のように、$f, g : S \to T$ とする。このとき、

$$f(s) = g(s)$$

と書いたら、「この特定の $s \in S$ について $f(s) = g(s)$ が成り立つ」ことを意味するのであるが、人によっては $f = g$ のことをこのように書くことがあり、紛らわしい。そこで、$f = g$ のことを $f(s) \equiv g(s)$ と書くこともある。

数学記号 $\forall$ (for all, for any の a の大文字の逆立ち) を用いれば

$$f(s) \equiv g(s) \Leftrightarrow f = g \Leftrightarrow \forall s \in S, f(s) = g(s)$$

である。ここで、最後の命題は「全ての $s \in S$ に対し、$f(s) = g(s)$ が成り立つ」と読む。

定義 1.1.9. 集合 S から集合 T への写像全体の集合を

$$\mathrm{Map}(S, T) := \{f \mid f : S \to T\}$$

であらわす。$\mathrm{Map}(S, T)$ を T^S とも記す。

定義 1.1.10. (合成写像)

$f : S \to T$, $g : T \to U$ なる二つの写像が与えられたとき、その合成写像 $g \circ f : S \to U$ を任意の $s \in S$ に対して

$$(g \circ f)(s) = g(f(s))$$

となる写像として定義する。

命題 1.1.11. (関数の合成の結合律)

上の状況で、さらに $h : U \to V$ なる写像があるとする。このとき、

$$h \circ (g \circ f) = (h \circ g) \circ f \tag{1.2}$$

が成立する (関数の合成に関する**結合律** associativity という。**結合法則**とも言う)。

証明. すべての $s \in S$ に対して

$$(h \circ (g \circ f))(s) = ((h \circ g) \circ f)(s)$$

を言えばよいが、両辺とも $h(g(f(s)))$ に一致するので言える。 □

問題 1.1. (1.2) の証明を完成せよ。

定義 1.1.12. （恒等写像）S を集合とする。id_S で、S から S への元を変えない写像を表す。すなわち、$\mathrm{id}_S : S \to S$ は次を満たす写像。

$$\forall s \in S,\ \mathrm{id}_S(s) = s.$$

id_S を S 上の**恒等写像** (identity map) と言う。

命題 1.1.13. (恒等写像の単位法則)
任意の $f : S \to T$, $g : U \to S$ に対して

$$f \circ \mathrm{id}_S = f, \quad \mathrm{id}_S \circ g = g$$

が成立する。

（こういう言い方をしたら、上のコンマで区切られた左右のそれぞれが同時に成り立つことを意味する。）

定義 1.1.14. $f : S \to T$ が $g : T \to S$ の逆写像（inverse map、逆射とも言う）であるとは、

$$g \circ f = \mathrm{id}_S, \ f \circ g = \mathrm{id}_T$$

が成り立つこと。
このとき、S の元の数と T の元の数は等しくなる。

平たく言えば、S の元を f で T に送って、次に g で S に送ると元に戻り (これが $g \circ f = \mathrm{id}_S$ と同値)、また T の元を g で送って f で送ると元に戻る (これが $f \circ g = \mathrm{id}_T$ と同値) ということである。

問題 1.2. $f : S \to T$, $g : T \to S$ であって

$$g \circ f = \mathrm{id}_S, \ f \circ g \neq \mathrm{id}_T$$

となるような例を作れ。

定義 1.1.15. $f : S \to T$ を写像とする。このとき、f による S の像 (image of f) とは、f によって S から来れる T の元の全体である。これを、$f(S)$ で表す。すなわち、

$$f(S) := \{f(s) \mid s \in S\}.$$

これは、T の部分集合である。すなわち、$f(S) \subset T$。

定義 1.1.16. $f : S \to T$ が全射 (surjection, epimorphism) であるとは、$f(S) = T$ が成立すること。言い換えれば、T のどの元も、f によって S の元から来ていること。
つまり、任意の $t \in T$ に対し、ある $s \in S$ がとれて $t = f(s)$ という形にかけることで、論理式で書けば

$$\forall t \in T, \exists s \in S, t = f(s).$$

注意 1.1.17. 上の論理式は、正確に書けば

$$\forall t \in T[\exists s \in S(t = f(s))]$$

と書くべきものである。これは、

「任意の $t \in T$ に対し、[ ] の中身が成り立つ」

ことを意味している。
数学では、同じ意味の数式を

$$[\exists s \in S(t = f(s))](\forall t \in T)$$

のように書いたりすることもある。

問題 1.3. もし、順序を入れ替えて

$$\exists s \in S[\forall t \in T(t = f(s))]$$

とすると、どういう意味になるか。（答 : S, T が空集合でないときには、T が一元集合であること。S または T が空集合の時には、どうなるでしょう。）

定義 1.1.18. 写像 $f : S \to T$, $g : T \to S$ が $f \circ g = \mathrm{id}_T$ を満たすとき、g は f の右逆写像である（right inverse map）という。f は g の左逆写像である（left inverse map）という。

命題 1.1.19. 写像 $f : S \to T$ が全射である必要十分条件は、ある $g : T \to S$ が存在して $f \circ g = \mathrm{id}_T$ となることである。すなわち、次が成立。

$$f \text{ が全射} \Leftrightarrow f \text{ が右逆写像を持つ。}$$

証明の前に、用語を一つ用意する。

定義 1.1.20. 写像 $f : S \to T$ を考える。$t \in T$ に対し、S の部分集合

$$f^{-1}(t) := \{s \in S \mid f(s) = t\}$$

を t の f による逆像 (inverse image) という。これは、「f で送ると t になるような S の元の集合」である。元 t に対応するのが、元ではなくて集合 $f^{-1}(t)$ であることを注意しておく。

この定義により、f が全射である必要十分条件は、「全ての $t \in T$ に対し $f^{-1}(t)$ が空でない」ことになる。

証明. (命題 1.1.19 の)
必要性 : 各 $t \in T$ に対し、$f^{-1}(t)$ から適当に一個元 s を選び出し、それを $g(t)$ と定義する。こうして作った $g : T \to S$ は、上の命題の条件 $f \circ g = \mathrm{id}_T$ を満たす。 □

問題 1.4. 十分性を示せ。(ヒント : たとえば問題 1.9 の 1 を使ってもできる。)

定義 1.1.21. $f : S \to T$ が単射 (injection, monomorphism) であるとは、「S の異なる元の f による像は、T の異なる元である」こと。
数式で言えば、

$$\forall s, s' \in S, s \neq s' \Rightarrow f(s) \neq f(s')$$

のこと。対偶を取って、

$$\forall s, s' \in S, f(s) = f(s') \Rightarrow s = s'$$

と言っても同じ。

命題 1.1.22. S を空でない集合とする。写像 $f : S \to T$ が単射である必要十分条件は、ある $g : T \to S$ が存在して $g \circ f = \mathrm{id}_S$ となること。すなわち、次が成立。

$$f \text{ が単射} \Leftrightarrow f \text{ が左逆写像を持つ。}$$

証明. f が単射であるということは、全ての $t \in T$ に対して集合 $f^{-1}(t)$ の元の数が 0 または 1 であるということである。そこで、それぞれの t に対し、$g(t) \in S$ を (1) もし $f^{-1}(t)$ に元があればその元とし、(2) そうでなければ T の元をなんでもいいからとり、それを $g(t)$ と定める（ここで、$S \neq \emptyset$ を使っている）。こうして得られた $g : T \to S$ は $g \circ f = \mathrm{id}_S$ を満たしている。これで必要性は示された。 □

問題 1.5. 十分性を示せ。

命題 1.1.23. $f : S \to T$ が右逆写像 g と左逆写像 g' を持てば、$g = g'$ となる。したがって g は f の逆写像となる。

証明. 右逆写像 $g : T \to S$ は $f \circ g = \mathrm{id}_T$ を満たす。左逆写像 g' は $g' : T \to S$ は $g' \circ f = \mathrm{id}_S$ を満たす。$g = g'$ を言えばよいが、これは結合律 (1.2) を用いて

$$g' = g' \circ \mathrm{id}_T = g' \circ (f \circ g) = (g' \circ f) \circ g = \mathrm{id}_S \circ g = g$$

により示される。 □

系 1.1.24. $f : S \to T$ が逆写像を持てば、それはただ一つである。

証明. $g, g' : T \to S$ を二つの逆写像とする。g は右逆写像であり、g' は左逆写像であるから、上の命題により $g = g'$ であり、ただ一つとなる。 □

定理 1.1.25. $f : S \to T$ が逆写像を持つ必要十分条件は、全射かつ単射であることである。

証明. 必要性は命題 1.1.19, 1.1.22 から従う。十分性については、命題 1.1.19 から f が右逆写像を持つことがわかり、命題 1.1.22 から f が左逆写像をもつことがわかるので、命題 1.1.23 から逆写像を持つことがわかる。 □

定義 1.1.26. 全射かつ単射であるような写像を、**全単射** (bijection) という。一対一対応 (one-to-one correspondence) ともいう。上の定理 1.1.25 により、これは「逆写像を持つこと」と同値である。

問題 1.6. 定理 1.1.25 の、より直接的な証明を与えよ。

命題 1.1.27. S, T を有限集合とする。$f : S \to T$ なる全単射があれば、$\#(S) = \#(T)$。

命題 1.1.28. $f : S \to T$ を単射とすると、$f : S \to f(S)$ は全単射である。よって特に T が有限集合の時は、$\#(S) = \#(f(S)) \leq \#(T)$、したがって

$$\#(S) \leq \#(T).$$

もしさらに $\#(S) = \#(T)$ ならば、$f : S \to T$ は全単射である。

証明. $\#(S) \leq \#(T)$ までは明らか。T が有限集合で $\#(S) = \#(T)$ であると仮定すると、$\#(f(S)) = \#(T)$ となり、$f(S) \subset T$ と合わせて $f(S) = T$。よって全射となる。 □

命題 1.1.29. $f : S \to T$ を全射とすると、$g : T \to S$ なる単射が存在する。よって特に S が有限集合の時は、$\#(T) \leq \#(S)$。もしさらに $\#(S) = \#(T)$ ならば、$f : S \to T$ は全単射である。

証明. 命題 1.1.19 により $f \circ g = \mathrm{id}_T$ なる $g : T \to S$ が存在し、命題 1.1.22 より g は単射。S が有限集合のとき直前の命題 1.1.28 を g に対して適用すると $\#(T) \leq \#(S)$。等号が成立するとき、同じ命題により g が全単射であることがわかる。f が g の逆射であることは $f \circ g = \mathrm{id}_T$ に右から g^{-1} を合成すればわかり、f は逆射をもつので全単射となる。 □

問題 1.7. $f : S \to T$ を全射とし、$g, g' : T \to U$ を二つの写像とする。

$$g \circ f = g' \circ f \Rightarrow g = g'$$

を示せ。（全射は右から消去できる、right cancellable という。）

問題 1.8. $f : S \to T$ を単射とし、$g, g' : R \to S$ を二つの写像とする。

$$f \circ g = f \circ g' \Rightarrow g = g'$$

を示せ。（単射は左から消去できる、left cancellable という。）

問題 1.9. $f : S \to T$, $g : T \to U$ とする。以下を証明せよ。

1. $g \circ f$ が全射ならば、g は全射
2. g, f が全射ならば、$g \circ f$ は全射
3. $g \circ f$ が単射ならば、f は単射
4. g, f が単射ならば、$g \circ f$ は単射

問題 1.10. S, T を有限集合とするとき、

$$\#(S \times T) = \#(S) \times \#(T)$$

を証明せよ。任意有限個の直積の場合はどうか？

問題 1.11. S, T を有限集合とするとき、

$$\#(T^S) = \#(T)^{\#(S)}$$

を証明せよ。

問題 1.12. （やや難）上の問題において、S や T が空集合である場合を考察することで、0^0 を 1 と定義することが妥当であることを導け。

問題 1.13. S を有限集合とするとき、

$$S^{\{1,2,\ldots,n\}} = S^n$$

を証明せよ。(S^n は定義 1.1.3 を参照。“=” というのはちょっとうそで、「同じものとみなすことができる」という微妙なニュアンスを表している。) 注 1.3.3 を参照。

問題 1.14. （Bernstein の定理 [1, p.63]。難しい問題に飢えた読者のために）
$f : S \to T$ なる単射と、$g : T \to S$ なる単射があれば、S から T への全単射が存在することを示せ。

1.1.4 直積と写像

S, T, U を集合とし、

$$f : S \times T \to U$$

なる写像を考える。$s \in S, t \in T$ に対して $f(s,t) \in U$ が定まるわけであるが、今 $s_0 \in S$ を一つ固定して、

$$t \in T \mapsto f(s_0, t) \in U$$

なる写像を考えると、これは $T \to U$ なる写像である。すなわち、

$$f_{s_0}(t) := f(s_0, t)$$

とおけば、f_{s_0} は $\mathrm{Map}(T, U)$ の元である。

ということは、$s_0 \mapsto f_{s_0}$ は

$$S \to \mathrm{Map}(T, U)$$

なる写像を与える。

逆に、$g : S \to \mathrm{Map}(T, U)$ なる写像が与えられれば、$g(s_0) : T \to U$ であり、$g(s_0)(t) \in U$ である。そこで、$f(s,t) := g(s)(t)$ とおけば f は $S \times T \to U$ なる写像を与える。

定理 1.1.30. 上の対応で、

$$\mathrm{Map}(S \times T, U) \to \mathrm{Map}(S, \mathrm{Map}(T, U))$$

なる全単射が得られる。

問題 1.15. 上の定理を証明せよ。

1.2 演算

定義 1.2.1. S を集合とする。S 上の**二項演算** (binary operation) とは、

$$S \times S \to S$$

なる写像のことである。

例 1.2.2. 例えば、$f(x,y) := x + y$ は $\mathbb{R} \times \mathbb{R} \to \mathbb{R}$ なる写像を与えるので、二項演算である。この二項演算は「和」と呼ばれている。以下、二項演算の例を上げる。かっこ内には、「二項演算に見えてそうでないもの」の例を上げる。

1. 自然数 $\mathbb{N}$ 上の和、積、冪　（差には「閉じていない」。この用語については、下の注意 1.2.3 を参照）
2. 整数 $\mathbb{Z}$ 上の和、差、積、（商には閉じていない。冪にも閉じていない。）
3. 実数 $\mathbb{R}$ 上の和、差、積、（商と冪は定義できないことがある。$1 \div 0$, $(-1)^{\pi}$ など。）
4. （実）行列の和、差、積

注意 1.2.3.

1. 集合 S が二項演算 $\circ$ に**閉じている**、とは、暗黙のうちに S を含むより大きな集合 T が存在し、T では二項演算 $\circ$ が（常識として）与えられていて、

$$s_1, s_2 \in S \Rightarrow s_1 \circ s_2 \in S$$

を満たすこと。例えば、整数の集合を T とすると、そこには差が定義されている。自然数の集合を S とすると、$1 - 4 = -3 \notin S$ なので「自然数は差に（ついて）閉じていない」という。

2. まれに、「集合 S のある部分集合 S_0 の元同士には演算 $\circ$ が定義されているが、S 全体には定義されない」ことを「S が演算 $\circ$ に閉じていない」ということがある。

   例えば、実数の全体 $\mathbb{R}$ をとり、二項演算として冪 a^b を考える。$(-1)^\pi$ のごときは、どう定義していいか、自然には決まらない。しかし、正の実数の集合 $\mathbb{R}_{>0}$ の元 a, b に対しては、a^b が定まることは高校で既習の通りである。

注意 1.2.4. 二項演算を表すのに、一つ記号（$\circ$ や $\times$ など）を定めて、二つの元の間にそれを書く方法

$$(a, b) \mapsto a \circ b$$

がもっとも多いが、時には a^b や $\frac{a}{b}$ のような例外もある。

1.2.1　n 項演算

集合 S が与えられたとき、S **上の単項演算** (unary operation) とは写像

$$S \to S$$

のことである。例として、S が整数のとき、x に対して $-x$ を対応させる写像は単項演算である。

一般に、S の n 個の直積から S への写像、すなわち $S^n = S \times S \times \cdots \times S \to S$ の形の写像のことを S **上の** n **項演算** (n-ary operation) という。

この定義に従うと、S **上の 0 項演算** (nullary, zeroary operation) とは

$$f : S^0 = \{()\} \to S$$

の形の写像のことである。これは、$f(()) \in S$ を決めることに他ならない。すなわち、S における 0 項演算を一つ決めることは、S の元を一つ決めることである。n 項演算が、「S の元を n 個もらって、それに応じて S の元を 1 個決める方法」であることから、0 項演算は「S の元を一つももらわずに S の元を 1 個決める方法」となり、単に「S の元を 1 個決める方法」となる。

1.2.2 より一般の演算

n 項演算の枠組みにおさまらない演算もたまにある。

線形空間の定義を（知っている人は）思い出そう。K を体 (§2.5) とする（体、という言葉を知らない人は K は実数の集合、または複素数の集合、どちらかと思っていていい)。

定義 1.2.5. 体 K 上の（抽象）線形空間 V とは、材料として

VA (台集合と呼ばれる) 集合 V_0

VB (和と呼ばれる)V_0 上の二項演算

VC (スカラー倍と呼ばれる) K の元 λ と V_0 の元 v に対して定まる $\lambda \circ v \in V_0$

であって、8 つの公理を満たすものをいう。（公理はここでは省略、例えば松坂 [2] 第 4 章参照。ただし本書でも定義 5.1.4 で与えられる。）

以後、V_0 と書くべきところを手抜きして V と書く。すると、スカラー倍と呼ばれる演算は、

$$K \times V \to V$$

の形の写像であり、通常の意味での二項演算ではない。

一般に、T, S を集合としたとき、

$$T \times S \to S$$

の形の写像を T の S への作用という (ことが多い)。この用語をつかえば、スカラー倍は K の V への作用である。

他にも、いろいろなタイプの演算がある。

例 1.2.6. 実ベクトル空間 $\mathbb{R}^n$ の内積 $\mathbf{x}, \mathbf{x}' \mapsto \mathbf{x} \cdot \mathbf{x}'$ は、

$$\mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$$

なる形の写像であり、今までの枠組みに入っていない。

例 1.2.7. S, T, U を集合とする。写像の合成は

$$\mathrm{Map}(T, U) \times \mathrm{Map}(S, T) \to \mathrm{Map}(S, U), \quad (g, f) \mapsto g \circ f$$

なる写像を与える。これも、演算と呼びたいところだが、今までの枠組みに入っていない。

一番広い定義をすると、

$$S_1 \times S_2 \times \cdots \times S_n \to T$$

の形の写像を全て演算といっても良い。が、本書では当面 §1.2.1 の意味での n 項演算のみを取り扱う。

問題 1.16. さまざまな演算の例を挙げよ。

1.3　同値関係と同値類

この章では同値関係を扱う。小学校で、$1/2 = 2/4 = 500/1000$ などと教わった。しかし、あらためて考えてみると、「$2/4 = 500/1000$ とはどういうことか？見た目からして全然違うじゃないか」と疑念がおきる。例えば、友人に「ピザを $2/4$ ください」と頼んで「ピザを 4 等分して 2 切れくれた」らうれしいが、「1000 等分して 500 切れくれた」ら衝撃である。実際小学校では「同じと思いなさい」と、「ごまかして」教えているとも言える。

以下に述べるように「同値関係」と「同値類」によって「同じと思う」という概念がより厳密に定義できる。

1.3.1　二項関係

定義 1.3.1. X を集合とする。X 上の**二項関係** (binary relation)R とは、$x_1, x_2 \in X$ に対して

$$x_1 R x_2$$

が成立するか否か（真であるか、偽であるか）が決められているもの。

例 1.3.2. 実数 $\mathbb{R}$ には大小関係とよばれる関係 $\geq$ が定義されている。$x_1 \geq x_2$ であるかないか、どちらかに定まるからである。

R が X 上の二項関係であるとき、

$$\mathcal{R} := \{(x_1, x_2) \in X \times X \mid x_1 R x_2\}$$

とおくと $X \times X$ の部分集合が定まる。これは、関係 R にある X の元のペアを全て集めたものである。逆に、$X \times X$ の部分集合 $\mathcal{R}$ を定めると、

$$x_1 R x_2 \Leftrightarrow (x_1, x_2) \in \mathcal{R}$$

により、X 上の二項関係 R が定まる。よって、X 上の二項関係と、$X \times X$ の部分集合とは、本質的に同じ概念である。

注意 1.3.3. **「本質的に同じ概念」**とはどういう意味であるか、定かでない。が、大抵は、次の状況を指す。

ある数学的対象の集合 $\mathcal{A}$ と、別の数学的対象の集合 $\mathcal{B}$ の間に、「自然な、誰が考えてもこれを一番に思いつくような、簡単な、良い、言い換えのような、当たり前の」一対一対応が存在する。

上の例で言えば、X を集合としたとき

$$\mathcal{A} = X \text{ 上の二項関係の集合}, \quad \mathcal{B} = X \times X \text{ の部分集合の集合}$$

であり、対応は $R \mapsto \mathcal{R}$ である。

「自然な」(natural, canonical) という部分は依然としてはっきりしない。おそらく、機械的な定義のできない、人間のセンスに依存したものなのだと思う。例を見ていくうちに納得いただけるといいなと思う。

上のように、二つの集合 $\mathcal{A}, \mathcal{B}$ の間に自然な一対一写像が唯一つ存在するとき、

$$\mathcal{A} = \mathcal{B}$$

と書いてしまうことも多い。例えば問題 1.13 のような場合である。

が、厳密には等しくないので区別したほうが良い。ここでは、

$$\mathcal{A} \overset{can}{\cong} \mathcal{B}$$

と記す。(**標準的に同型**, **canonically isomorphic** という。「同型」という言葉に違和感があると思うが、カテゴリー論の用語であり、ここではさらっと流してほしい。)

1.3.2 集合の分割と同値関係

集合 X を、互いに交わらない空でない部分集合に分割することを考える。例えば $\mathbb{N}$ は、偶数の集合と奇数の集合に分割される。この状況を、

$$\mathbb{N} = \text{偶数の集合} \coprod \text{奇数の集合}$$

であらわす。$\coprod$ は $\bigcup$ と似た意味の記号であるが、$\coprod$ でつながれた集合に共通部分がないことをも意味する記号で、(集合の) **直和** (direct sum)、あるいは**分離和**, **非交和** (disjoint union) と言う。以下の定義 1.3.4 で説明する。

他の例として、$\mathbb{N}$ は、3 で割った余りが 0 であるものの集合 C_0, 1 であるものの集合 C_1, 2 であるものの集合 C_2 に分割される。この状況は

$$\mathbb{N} = \coprod_{i=0,1,2} C_i$$

で表される。

無限個に分割されることもありうる。$\mathbb{C}$ を、絶対値で分類して

$$C_r := \{z \in \mathbb{C} \mid |z| = r\}$$

とおけば, C_r (r は $0 \leq r$ の範囲の実数を全部動く) は $\mathbb{C}$ の分割を与える。この状況は

$$\mathbb{C} = \coprod_{r \in \mathbb{R}, r \geq 0} C_r$$

で表される。

定義 1.3.4. X, I を集合とする。X の I で添え字づけられた**部分集合族** C_i $(i \in I)$ とは、各 $i \in I$ に対し C_i なる X の部分集合が定められたものを表す。X の部分集合族 C_i $(i \in I)$ が X の**被覆**であるとは、

$$X = \bigcup_{i \in I} C_i$$

が成り立つこと。C_i $(i \in I)$ が直和であるとは、任意の $i, j \in I, i \neq j$ に対して $C_i \cap C_j = \emptyset$ が成り立つこと。直和であるときには、それを明示するために $\bigcup_{i \in I} C_i$ を

$$\coprod_{i \in I} C_i$$

と書くことがある。C_i $(i \in I)$ が X の**分割** (partition) であるとは、X の被覆でかつ直和、かつ全ての $i \in I$ について $C_i \neq \emptyset$ であること。

C_i の一つ一つをこの分割の**類** (class) という。

注意 1.3.5. I が何なのか定かでなく思えるかも知れない。が、着目する X の部分集合たちに名前をつけるための名前の集合だと思っていい。上の例で言えば, 3 で割った余りの場合には $I = \{0, 1, 2\}$ であるし、複素数を絶対値の大きさで分割した場合には $I = \{r \in \mathbb{R} | 0 \leq r\}$ である。なお、I は index(見出し) の頭文字である。C_i の C は class の C。

さて、本節の主目的は「分割」と「同値関係」の間の自然な一対一対応を示すことである。

定理 1.3.6. （分割から同値関係を構成する）

X の分割 C_i $(i \in I)$ が与えられたとする。

$$x_1 \sim x_2 \Leftrightarrow x_1 \text{ と } x_2 \text{ が同じ類に属す} \tag{1.3}$$

によって二項関係 $\sim$ を定義すると、同値関係の公理（下の [E1][E2][E3]）を満たす。これを**分割に付随した同値関係**という。

定義 1.3.7. X 上の二項関係 R が**同値関係** (equivalence relation) であるとは、次の三つをみたすこと。

E1 推移律 aRb かつ bRc ならば aRc

E2 反射律 aRa

E3 対称律 aRb ならば bRa

(なお、R を同値関係としたとき、aRb のことを a と b は R に関して同値であるという。)

証明. (定理 1.3.6 の.) E1. aRb かつ bRc とする。aRb よりある $i \in I$ が存在して $a, b \in C_i$。bRC よりある $j \in I$ が存在して $b, c \in C_j$. $b \in C_i \cap C_j$ となるから、分割の直和性より $i = j$。したがって $a, c \in C_i$。よって aRc。E2. 分割の被覆性よりある $i \in I$ が存在して $a \in C_i$。よって $a, a \in C_i$。よって $a \sim a$。E3. aRb ならば $i \in I$ が存在して $a, b \in C_i$。よって $b, a \in C_i$。よって bRa。 □

このように、分割から同値関係が構成される。逆に、同値関係 R が与えられたとき、互いに同値関係にあるような X の元同士を集めて類をつくると、X の分割が与えられる。

定義 1.3.8. (同値類)

$(X, \sim)$ を集合とその上の同値関係とする。$(X, \sim)$ における同値類 (equivalence class) C とは、X の部分集合 $C \subset X$ であって

C1 C は空でない

C2 $x_1, x_2 \in C$ ならば $x_1 \sim x_2$

C3 $x_1 \in C$ かつ $x_1 \sim x_3$ ならば $x_3 \in C$

を満たすもののこと。

命題 1.3.9. $(X, \sim)$ を集合とその上の同値関係とする。$x \in X$ に対して

$$C_x := \{y \in X \mid x \sim y\}$$

と定義すると、C_x は x を含むただ一つの同値類である。また、C を一つの同値類とする。同値類の定義より、C は空でない。したがって $x \in C$ を一つとることができる。このとき、

$$C = C_x$$

である。

証明. C_x が同値類であること：C1. 反射律より $x \in C_x$、よって空ではない。C2. $x_1, x_2 \in C_x$ ならば定義より $x \sim x_1$, $x \sim x_2$ 対称律より $x_1 \sim x$。これに推移律を用いて $x_1 \sim x_2$。C3. $x_1 \in C_x$ かつ $x_1 \sim x_3$ ならば、$x \sim x_1$ と推移律を用いて $x \sim x_3$、よって $x_3 \in C_x$。これで同値類と言えた。

$x \in C$ ならば $C = C_x$ であること：$y \in C$ ならば C2 より $x \sim y$、よって $y \in C_x$、すなわち $C \subset C_x$。また、$y \in C_x$ ならば $x \sim y$ で C3 より $y \in C$、すなわち $C_x \subset C$。よって $C = C_x$ と言えた。 □

定義 1.3.10. 上の命題の C_x を $[x]$ または $\bar{x}$ で表し、x が**属する同値類**、または x の同値類という。

定理 1.3.11. (同値関係から分割を構成する)
$(X, \sim)$ を集合とその上の同値関係とし、C_i $(i \in I)$ をそれが与える同値類の集合とすると、これは X の分割となる。

証明. 被覆であること：任意の $x \in X$ が同値類 $[x]$ に含まれるので、同値類の集合は被覆である。直和であること：C_i と C_j に共通の元が x が存在するとすると仮定する。命題 1.3.9 より $C_i = [x] = C_j$ となる。空でないこと：同値類の定義から空でない。 □

定理 1.3.12. 定理 1.3.6 により、X の分割から X 上の同値関係が構成できる。逆に、同値関係から上の定理により X の分割が構成できる。この対応により、

$$X \text{ 上の同値関係の集合} \to X \text{ の分割の集合}$$

なる、自然な一対一対応が得られる。

証明. 定理 1.3.6、定理 1.3.11 の証明を追うと、互いに逆であることを確かめることができる。それは読者にまかせる。証明よりも大事なかもしれない注意として、「二つの分割 $C_i(i \in I)$ と $C'_j(j \in J)$ が同じである」ということを明確化しておく。集合として $\{C_i \mid i \in I\} = \{C'_j \mid j \in J\}$ が成立するとき、これらの分割を「同じ」という。 □

この意味で、X 上に同値関係を一つ与えることと、X の分割を一つ与えることとは同じことである。(「同じこと」とはどういうことかについては、注 1.3.3 を参照のこと。)

定義 1.3.13. 上の定理 1.3.11 において、同値類の集合を

$$X/\sim$$

と表し、X の $\sim$ による**商集合** (quotient set) という。これは、X の同値類の一つ一つを一点につぶして得られる集合である。

全射

$$q : X \to X/\sim, \quad x \mapsto [x]$$

を**商写像** (quotient map) という。

同値関係の定義と同値類の定義から、

$$x \sim y \Leftrightarrow y \in [x]$$

および

$$x \sim y \Leftrightarrow [x] = [y]$$

が成立する。

例 1.3.14. X を、ある学校の生徒の集合とし、$x_1 \sim x_2$ を「x_1 と x_2 は友達である」という関係だとする。ここで、「人は自分とは友達である」ということにして、さらに「友達の友達は友達である」「a と b が友達なら、b と a は友達である」と仮定すると、$\sim$ は同値関係となる。x の友達の集合が、同値類 $[x]$ となる。

X は、同値類=「友達グループ」に分割される。$X/\sim$ は、友達グループの集合となる。自分以外の友達がいない人 x の友達グループは $[x] = \{x\}$ となる。

例 1.3.15. (**写像の与える同値関係**・重要)

写像があると、その始集合に次のような同値関係が与えられる。X, Y を集合とし、$f : X \to Y$ を写像とする。このとき、X 上の二項関係 $\sim_f$ を

$$x_1 \sim_f x_2 \Leftrightarrow f(x_1) = f(x_2)$$

で与えると、これは同値関係になる。この同値関係による X の分割は、

$$X = \coprod_{y \in f(Y)} f^{-1}(y)$$

となる。

問題 1.17. 例 1.3.15 の $\sim_f$ が同値関係になること、および対応する分割が上のようになることを証明せよ。

逆に、X 上に同値関係 $\sim$ が与えられたとき、上のような Y, $f : X \to Y$ を構成して $\sim = \sim_f$ とすることが可能である。$Y := X/\sim$, $f = q$ とすればよい。(後述の定理 1.3.33 の (1)。)

1.3.3　同値関係と写像のコンパチビリティ

この、「写像と同値関係とのコンパチビリティ」というのは、適切な日本語訳のない概念で、わかりにくいとよく言われる。が、名前がわかりにくいだけで定義はシンプルである。

定義 1.3.16. （写像と同値関係とのコンパチビリティ）

$f : X \to Y$ を写像とし、$(X, \sim)$ を同値関係とする。このとき、f と $\sim$ がコンパチブルであるとは、$x \sim y \Rightarrow f(x) = f(y)$ が成立することである。

このとき、X の同値類 C に対し、$x \in C$ の選び方によらず $f(x)$ は (C のみに依存した) 一定の値になる。よって、各 C に対して f の値は一定に定まるから、$X/\sim$ から Y への写像が定まる。この写像を $\bar{f} : X/\sim \to Y$ と書き、f から誘導される写像という。後述の定理 1.3.20 でより詳しく述べる。

有理数の例

少し具体的な例

$$f : \mathbb{Z} \times \mathbb{N} \to \mathbb{Q}, \quad (n, m) \mapsto \frac{n}{m}$$

を考えてみる。例 1.3.15 により、$\sim_f$ なる同値関係が $\mathbb{Z} \times \mathbb{N}$ に入る。これは、具体的には

$$(n, m) \sim_f (n', m') \Leftrightarrow \frac{n}{m} = \frac{n'}{m'}$$

で与えられる。

さて、有理数とはそもそも何であったか。小学校のころ習ったのは、(負の数は入っていなかったが)「$\frac{n}{m}$ なるものの全体であり、ただし通分して同じになるものは同じ数と思う」というものであった。この「同じものと思う」という操作が、商集合をとるという操作に他ならない。

例 1.3.17. 自然数 $\mathbb{N}$ や整数 $\mathbb{Z}$ は既知のものとして、ここから有理数を作る操作は商集合

$$(\mathbb{Z} \times \mathbb{N})/\sim,$$

をとることである。ここに同値関係 $\sim$ は

$$(n, m) \sim (n', m') \Leftrightarrow nm' = n'm$$

で定義する。

定義 1.3.18. 有理数の集合とは、上の例にある

$$(\mathbb{Z} \times \mathbb{N})/\sim,$$

のことである。(n, m) の属する類 $[(n, m)]$ のことを $\frac{n}{m}$ と表記する。

上の定義から自然に $\frac{1}{2} = \frac{2}{4}$ が従う。なぜならば、この等式は $[(1, 2)] = [(2, 4)]$ に他ならないが、$1 \cdot 4 = 2 \cdot 2$、すなわち $(1, 2) \sim (2, 4)$ から直ちに従う。

1.3.4 Well-definedness

上のようにして定義された有理数の集合

$$\mathbb{Q} := \mathbb{Z} \times \mathbb{N}/\sim$$

に対し、演算や写像を定義したいとする。小学校では、例えば和と呼ばれる二項演算を

$$\frac{n}{m} + \frac{n'}{m'} = \frac{nm' + n'm}{mm'} \tag{1.4}$$

と定義する、と習う。しかし、実はこれが「ちゃんと定義になっている」(=well-defined) ことを示す必要がある。

例えば今、$\mathbb{Q}$ 上の二項演算 $*$ を

$$\frac{n}{m} * \frac{n'}{m'} = \frac{n+n'}{m+m'}$$

で定義したとしよう。すると、

$$\frac{1}{2} * \frac{1}{3} = \frac{2}{5}$$

だが、

$$\frac{2}{4} * \frac{1}{3} = \frac{3}{7}$$

であり、$\frac{1}{2} = \frac{2}{4}$ に矛盾する。

もっと簡単な例を挙げる。

例 1.3.19. 写像

$$\mathbb{Q} \to \mathbb{Z}, \frac{n}{m} \mapsto n \text{ を } m \text{ で割った商}$$

を考える。これはちゃんと写像になっている (切り上げと呼ばれる、$\frac{n}{m}$ 以上の最小の整数である) のだが、

$$\mathbb{Q} \to \mathbb{Z}, \frac{n}{m} \mapsto n \text{ を } m \text{ で割った余り}$$

というのは写像を定義しない。$\frac{1}{2} = \frac{2}{4}$ であるが、$\frac{1}{2} \mapsto 1$ なのに、$\frac{2}{4} \mapsto 2$ だからである。

定理 1.3.20. (**well-definedness**) $(X, \sim)$ を集合とその上の同値関係とし、$q : X \to X/\sim$ を商写像とする。$f : X \to Y$ を任意の写像とする。

写像 $h : X/\sim \to Y$ であって、

$$f = h \circ q$$

なる性質をもつものが存在する必要十分条件は、任意の $x, x' \in X$ に対し

$$x \sim x' \Rightarrow f(x) = f(x')$$

となることである。このとき、h はただ一つに決まる（しばしば $\bar{f}$ で表される。）

この状況を、**写像 f は同値関係 $\sim$ とコンパチブル** であるといい (注：すでに定義 1.3.16 でこの用語を導入している)、また $\bar{f}$ が **well-defined** であるという。

この定理の意味と証明は、次のとおりである。X は良くわかっている集合とする。今、商集合 $X/\sim$ から Y への写像 h を定義したい。X はわかっているので、$f : X \to Y$ なる写像を定義することで、$\bar{f} : X/\sim \to Y$ を定義したい。$\bar{f}$ と f との関係は、

$$\bar{f}([x]) = f(x) \tag{1.5}$$

となるようにしたい。$q(x) := [x]$ であったから、

$$\bar{f} \circ q = f \tag{1.6}$$

と言っても同じである。このような $\bar{f}$ が存在すると仮定すると、$[x] = [x']$ ならば $\bar{f}([x]) = \bar{f}([x'])$ であるから (1.5) より $f(x) = f(x')$ であることが必要である。言い換えるとコンパチビリティ：「任意の $x, x' \in X$ に対して

$$x \sim x' \Rightarrow f(x) = f(x')$$

が成立すること」が必要である。逆に、コンパチビリティを仮定する。C を任意の同値類とする。$x \in C$ ならば $C = [x]$ であり、$\bar{f}([x]) = f(x)$ となるためには $\bar{f}(C) = f(x)$ であり、$\bar{f}(C)$ は存在するなら $f(x)$ と決めるしかない。これで一意性が言える。さらに $f(x)$ は $x \in C$ の選び方によらないことが次のようにしてわかる。C から他に $x' \in C$ を選んだとき、$x \sim x'$ なのでコンパチビリティにより $f(x) = f(x')$。したがって、f は C 上で一定の値をとる。この値を $\bar{f}(C)$ と決める。任意に $y \in X$ をとる。$f(y) = \bar{f}([y]) = f \circ q(y)$ となったので、$\bar{f} \circ q = f$ となった。（証明終わり。）

上の切り上げの例 1.3.19 では、

$$X = \mathbb{Z} \times \mathbb{N}$$

であり、

$$f(n, m) = n \text{ を } m \text{ で割った商}$$

である。この商を $q = f(n, m)$ としよう。すなわち、

$$n = mq + r, \quad 0 \leq r < m.$$

すると、

$$(n, m) \sim (n', m')$$

ならば

$$n' = (nm')/m = (mqm' + rm')/m = m'q + rm'/m$$

である。$n', m'q$ は整数だから rm'/m も整数で、$0 \leq rm'/m < m'$ だから、n' を m' で割った商 $f(n', m')$ は $q = f(n, m)$ で、余りは rm'/m である。

よって、

$$(n, m) \sim (n', m') \Rightarrow f(n, m) = f(n', m')$$

すなわち定理 1.3.20 の意味で f は well-defined であり、

$$\bar{f} : \mathbb{Z} \times \mathbb{N}/\sim \to \mathbb{Z}$$

であって $\bar{f}([n, m]) = f(n, m)$ となるものが存在する。

問題 1.18. 上で、「n を m で割った商」を「n を m で割った余り」に取り替えると、well-defined にならないことを示せ。

上の定理 1.3.20 で、Y を $Y/\sim_Y$ に取り替えると、次の定理を得る。

定理 1.3.21. (well-definedness) $(X, \sim_X)$, $(Y, \sim_Y)$ を集合とその上の同値関係とする。$q_X : X \to X/\sim_X$, $q_Y : Y \to Y/\sim_Y$ を商写像とする。

$f : X \to Y$ を任意の写像とする。写像 $h : X/\sim_X \to Y/\sim_Y$ であって、

$$q_Y \circ f = h \circ q_X$$

なる性質をもつものが存在する必要十分条件は、

$$x \sim_X x' \Rightarrow f(x) \sim_Y f(x')$$

となることである。このとき、h はただ一つに決まる（しばしば $\bar{f}$ で表される。）

この状況を、写像 f は同値関係 $\sim_X$, $\sim_Y$ にコンパチブルであるといい、$\bar{f}$ が well-defined であるという。

証明は読者にゆだねる。次の命題の証明も読者にまかせる。

命題 1.3.22. $(X, \sim_X), (Y, \sim_Y), (Z, \sim_Z)$ を三つの集合とその上の同値関係とする。$q_X : X \to X/\sim_X$, $q_Y : Y \to Y/\sim_Y$, $q_Z : Z \to Z/\sim_Z$, を商写像とする。
$f : X \times Y \to Z$ を写像とするとき

$$\bar{f} : X/\sim_X \times Y/\sim_Y \to Z/\sim_Z$$

であって、任意の $x \in X, y \in Y$ に対し

$$\bar{f}(q_X(x), q_Y(y)) = q_Z \circ f(x, y)$$

を満たすものが存在する必要十分条件は、任意の $x, x' \in X$, $y, y' \in Y$ に対して

$$x \sim_X x', \quad y \sim_Y y' \Rightarrow \quad f(x, y) \sim_Z f(x', y')$$

が成立すること。このことを f は $\sim_X, \sim_Y, \sim_Z$ とコンパチブルであるといい、また $\bar{f}$ が well-defined であるという。このとき $\bar{f}$ はただ一つに定まる。

この命題において $X = Y = Z = S$ とすると、f は二項演算となり、次の系が得られる。この系は「集合 S 上の同値関係と二項演算がコンパチブルならば、X の商集合に自然に二項演算を誘導する」ことを主張する。

系 1.3.23. (**二項演算と同値関係のコンパチビリティ**)
$(S, \circ)$ を集合と二項演算とする。$\sim$ を S 上の同値関係とする。このとき、$S/\sim$ 上の二項演算 $\bar{\circ}$ であって (全ての $s_1, s_2 \in S$ に対して)

$$[s_1]\bar{\circ}[s_2] = [s_1 \circ s_2]$$

なるものが存在する必要十分条件は、

$$s_1 \sim s_1', s_2 \sim s_2' \Rightarrow s_1 \circ s_2 \sim s_1' \circ s_2'$$

となることである。(ここに $[s]$ は $s \in S$ の属する $S/\sim$ の元 (同値類) をあらわす、定義 1.3.13 参照。) この条件を満たすとき、$\circ$ と $\sim$ は**コンパチブル**であるといい、$\bar{\circ}$ は well-defined であるという。$\bar{\circ}$ はただ一つに決まる。

問題 1.19. 例 1.3.17 において $X := \mathbb{Z} \times \mathbb{N}$ 上の二項演算 $\tilde{+}$ を

$$(n, m)\tilde{+}(n', m') := (nm' + n'm, mm')$$

で定義すると、これは系 1.3.23 の意味で $\sim$ とコンパチブルであり、従って

$$\mathbb{Q} = (\mathbb{Z} \times \mathbb{N})/\sim$$

上の二項演算を定義することを示せ。(これが、分数の足し算の定義である。)

1.3.5 合同類

有理数の他に、数学に現れる典型的な同値類として m を法 (modulo) とする合同類、別名剰余類があげられる。

定義 1.3.24. m を整数とする。$x, y \in \mathbb{Z}$ に対し、x と y が m を法として**合同**であるとは、$x-y$ が m で割り切れることをいう。このとき

$$x \equiv y \bmod m$$

または

$$x \equiv_m y \tag{1.7}$$

とあらわす。これは $\mathbb{Z}$ 上の同値関係となる。この同値関係による同値類を、m を法とする**合同類** (congruence class) または**剰余類** (residue class) という。

念のために、「割り切れる」ことの定義を再確認する。n, m を整数としたとき、「n が m で割り切れる」とは、「ある整数 a が存在して $n = am$ となる」ことを言う。「n が m の倍数である」と言っても同値である。特に $a = 0$ ととることにより、0 は m の倍数の一つである。$m, 2m, 3m, \ldots$ 同様、$-m, -2m, -3m, \ldots$ はどれも m の倍数である。

問題 1.20. 上の合同関係は、同値関係であることを示せ。

定義 1.3.25. $x \in \mathbb{Z}$ と $m \in \mathbb{N}$ に対し、

$$x = mq + r, \quad 0 \leq r < m$$

となるような整数 q と r が唯一つ存在する。q を x を m で割った商 (quotient)、 r を余り (residue) という。商に文字 q, 余りに文字 r を良く使うのはこうした事情による。

問題 1.21. このような整数 q と r が存在すること、および唯一つであることを示せ。

例 1.3.26. -1 を 7 で割った余りは 6 である。

$$-1 = 7 \times (-1) + 6$$

だから。

定義 1.3.27. m を自然数とする。$x \in \mathbb{Z}$ に対し、x を m で割った余りを $r_m(x)$ と記す。r_m は

$$r_m : \mathbb{Z} \to \{0, 1, 2, \ldots, m-1\}$$

なる全射である。

命題 1.3.28. 上の状況で、

$$x \equiv y \bmod m \Leftrightarrow x \sim_{r_m} y$$

($\sim_f$ は、写像 f が与える同値関係である。例 1.3.15 を参照)。

これは、$x - y$ が m で割り切れる必要十分条件が、x を m で割った余りと y を m で割った余りとが一致することである、ということを数式で書いたに過ぎない。

問題 1.22. 上の命題を証明せよ。

命題 1.3.29. m を自然数とし、$\equiv_m$ を m を法とする合同関係とする。このとき、

$$\mathbb{Z}/\equiv_m \to \{0, 1, 2, \ldots, m-1\}$$

なる自然な全単射がある。これにより、$\mathbb{Z}/\equiv_m$ と $\{0, 1, 2, \ldots, m-1\}$ を同一視 (注 1.3.3 参照) する。

定義 1.3.30. $\mathbb{Z}/\equiv_m$ を $\mathbb{Z}/m$ または $\mathbb{Z}/m\mathbb{Z}$ であらわす。

証明. $(\mathbb{Z}, \equiv_m)$ と $r_m : \mathbb{Z} \to \{0, 1, 2, \ldots, m-1\}$ は定理 1.3.20 の条件を満たすので、

$$\bar{r}_m : \mathbb{Z}/\equiv_m \to \{0, 1, 2, \ldots, m-1\}$$

なる写像を誘導する。これは、x の属する合同類 $[x]$ に対し、$r_m(x)$ を対応させる写像である。r_m が全射なので、$\bar{r}_m$ も全射である。単射性を示す。$\bar{r}_m([x]) = \bar{r}_m([y])$ と仮定して、$[x] = [y]$ を導けばよい。が、定理 1.3.20 より

$$r_m(x) = \bar{r}_m([x])$$

なので

$$r_m(x) = \bar{r}_m([x]) = \bar{r}_m([y]) = r_m(y)$$

よって $x \sim_{r_m} y$。命題 1.3.28 より $x \equiv_m y$、よって $[x] = [y]$。 □

定義 1.3.31. (代表系) $(X, \sim)$ を集合と同値関係とする。$X/\sim$ の各元（すなわち同値類）に対し、それに属する元 $a \in X$ を一個任意に選ぶ。これら選ばれた元を集めて得られる集合 R を $(X, \sim)$ の一つの代表系 (representative system) という。

このとき、写像 $r \mapsto [r]$ により、$R \to X/\sim$ なる全単射が得られる。

例 1.3.32. 命題 1.3.29 で扱われた $(\mathbb{Z}, \equiv_m)$ に対し、$\{0, 1, \ldots, m-1\}$ は一つの代表系である。また、$\{-m, -m+1, \ldots, -1\}$ も一つの代表系である。

問題 1.23. $\mathbb{Z}$ における二項演算である和、積、差はそれぞれ m を法とする合同関係とコンパチブルであり、したがって系 1.3.23 の意味で $\mathbb{Z}/m$ における二項演算を定めることを示せ。

これにより、$\mathbb{Z}/m$ には「環」と呼ばれる代数構造が入る（後述、定義 2.5.1）。

問題 1.24. $\mathbb{Z}$ における単項演算 $x \mapsto |x|$ は $\mathbb{Z}/m$ における単項演算を定理 1.3.21 の意味で定めるか？

1.3.6　集合の準同型定理

命題 1.3.29 は、一般の同値関係に対し次の定理の後半のように一般化される。

定理 1.3.33. (集合の準同型定理)

1. $(X, \sim)$ を集合とその上の同値関係とする。商写像

$$q : X \to X/\sim$$

に対し、例 1.3.15 のように $\sim_q$ を定義すると、$\sim = \sim_q$ である。

2. $f : X \to Y$ なる写像が与えられたとする。$f(X) \subset Y$ で f による X の像を表す。このとき、f が

$$X \overset{q}{\to} X/\sim_f \overset{\bar{f}}{\to} Y$$

なる合成となるような $\bar{f}$、すなわち

$$f = \bar{f} \circ q$$

なる $\bar{f}$ がただ一つ存在する。そして、$\bar{f}$ の終集合を $f(X)$ に制限して得られる

$$\bar{f} : X/\sim_f \to f(X)$$

は全単射となる。

証明は、あたりまえな気がするまで自分で考えてみること。

問題 1.25. 定理 1.3.33 を用いて命題 1.3.29 を証明せよ。

第2章　マグマ、半群、モノイド、群

二項演算が指定された集合を、マグマという。その演算が「結合法則」を満たすときに半群という。さらに、「単位元」が存在するときに、モノイドという。さらに、「任意の元に対して逆元が存在する」とき、群という。これらは、比較的シンプルな「代数構造」の例である。この章では、これらの概念をひとつひとつ段階的に扱う。

実際、数の概念の発達の歴史は、次のようにこれらのステップに沿っている。自然数の集合は加法についてマグマであり、結合法則を満たすので半群である。この集合には「単位元」がないが、「0」を付け加えて（0の発見）「0以上の整数の集合」とすると、0が単位元となり、モノイドとなる。この集合に、逆元を付け加えると「負の数」が生まれ（負の数の発見）、整数の集合という「群」が生まれる。

群を扱う代数系の教科書の多くは、マグマ、半群、モノイドを扱わない。しかし、現代の数学・情報科学には、しばしば半群やモノイドが登場する。例えば、情報科学の基礎であるオートマトン理論の「語」の概念は「自由モノイド」と一致する。また、数学における「カテゴリー」の概念はモノイドの一般化である。群の重要性は飛びぬけているとしても、現代数学を学ぶ上ではモノイドも重要と思える。

また、筆者自身が群を勉強したとき、「なぜ群をこのように定義するのか」「なぜ準同型をこのように定義するのか」という疑問につまづいた。本書では、群の解説を行う前に、群よりも条件が弱いマグマ、半群、モノイドを解説することで、これらの定義の自然さを納得できるように配慮した。なお、ブルバキ（フランスの数学者集団）の代数の教科書 [3] も、マグマ・半群・モノイドを扱っている。

2.1　マグマ

2.1.1　マグマとマグマ準同型

集合と二項演算の組を、マグマという。

定義 2.1.1. **マグマ** (magma) とは、集合 S と、S 上の二項演算

$$\circ : S \times S \to S$$

の組 $(S, \circ)$ のこと。二項演算 $\circ$ を S **にマグマの構造を与える演算**という。単に、$\circ$ を「マグマ $(S, \circ)$ の構造」ということもある。S をマグマ $(S, \circ)$ の**台集合** (underlying set) という。

例えば $(\mathbb{Z}, \times)$, $(\mathbb{Z}, -)$, $(\mathbb{N}, +)$, $(\mathbb{N}, \text{ベキ})$ などは、マグマの例である。

問題 2.1. $(\mathbb{N}, -)$, $(\mathbb{Z}, \text{ベキ})$ はマグマでないことを示せ。

注意 2.1.2. マグマの定義は、集合と二項演算の組 $(S, \circ)$ である。だが、「二項演算の指定された集合をマグマという」という定義をしばしばする。後者の定義だと、「マグマは集合である」ことになり、「台集合」という言葉の意味が不明瞭になる。本書では、なるべく前者の立場をとる。

注意 2.1.3. マグマは、昔は亜群 (groupoid) とも呼ばれていた。 が、今は通常亜群と言ったら別のもの（全ての射が可逆であるようなカテゴリー）を指すことが多い。

定義 2.1.4. (マグマの準同型) $(S, \circ_S)$, $(T, \circ_T)$ を二つのマグマとする。$(S, \circ_S)$ から $(T, \circ_T)$ への**マグマ準同型** (magma homomorphism)f とは、写像 $f : S \to T$ であって

$$\forall s, s' \in S, \quad f(s \circ_S s') = f(s) \circ_T f(s') \tag{2.1}$$

が成り立つもののこと。文脈から明らかなときは、単に「準同型」という。

注意 2.1.5. 上の条件を、「f は演算 $\circ$ を保存する」「f は演算 $\circ$ を保つ」(f preserves $\circ$) と言う。 $\circ$ と書いて、$\circ_S$ と $\circ_T$ の二つを同時に表しており、初めて見ると混乱する。

例 2.1.6. $a \in \mathbb{N}$ に対し、

$$L_a : \mathbb{N} \to \mathbb{N}, \quad x \mapsto ax$$

と定義する。L_a が $(\mathbb{N}, +)$ から $(\mathbb{N}, +)$ へのマグマ準同型かどうかは、

$$L_a(x + x') = L_a(x) + L_a(x')$$

が (全ての $x, x' \in \mathbb{N}$ について) 成り立つかどうかと同値であるが、これは分配法則

$$a(x + x') = ax + ax'$$

と同値であり、従って L_a は $(\mathbb{N}, +)$ から $(\mathbb{N}, +)$ へのマグマ準同型である。

一方、同じ L_a が $(\mathbb{N}, \times)$ から $(\mathbb{N}, \times)$ への準同型であるかどうかを考えてみる。準同型である条件を書き下すと、

$$L_a(x \times x') = L_a(x) \times L_a(x')$$

となる。が、左辺は axx'、右辺は $axax'$ である。これが任意の自然数 x, x' に対して成立する必要十分条件は、$a = a^2$ である。自然数の範囲では $a = 1$ のみが該当し、$a = 1$ であれば L_a はマグマ準同型、さもなければマグマ準同型ではない。

問題 2.2. $a \in \mathbb{N}$ とする。写像 $x \mapsto a^x$ は、$(\mathbb{N}, +)$ から $(\mathbb{N}, \times)$ のマグマ準同型を与えることを示せ。

定義 2.1.7. 可換図式。等式 (2.1) を、次のような図式（可換図式、commutative diagram）で表す。

$$\begin{array}{ccc} S \times S & \overset{f \times f}{\to} & T \times T \\ \downarrow \circ_S & \circlearrowright & \downarrow \circ_T \\ S & \overset{f}{\to} & T. \end{array}$$

これでは定義になっていないので、順に説明する。まず、

$$f \times f : S \times S \to T \times T$$

は、$(s, s') \mapsto (f(s), f(s'))$ で定義された写像である。上から下へ向かう二つの写像は、マグマの二項演算である。図式の真ん中の $\circlearrowright$ は、この図式が可換であること、すなわち左上の任意の元を、右上経由で右下に送っても、左下経由で右下に送っても、同じものになることを意味している。

左上の元を (s, s') としたとき、右上に送ると $(f(s), f(s'))$ であり、そこから右下に送ると $f(s) \circ_T f(s')$ となる。一方、同じ元を左下に送ると $s \circ_S s'$、そこから右に送ると $f(s \circ_S s')$ となる。この図式が可換であるとは、この両者が一致すること、すなわち (2.1) に他ならない。

命題 2.1.8. $(S, \circ_S)$、$(T, \circ_T)$、$(U, \circ_U)$ をマグマとし、$f : S \to T$, $g : T \to U$ をマグマ準同型とすると、合成

$$g \circ f : S \to U$$

もマグマ準同型である。これを、準同型の合成 (composition of homomorphisms) という。

証明. 言うべきことは

$$(g \circ f)(x \circ_S x') = (g \circ f)(x) \circ_U (g \circ f)(x')$$

だが、

$$g \circ f(x \circ_S x') = g(f(x \circ_S x')) = g(f(x) \circ_T f(x')) = g(f(x)) \circ_U g(f(x'))$$

より言える。一つ目の等号は関数の合成の定義、二つ目は f が準同型であること、三つ目は g が準同型であることより。 □

注意 2.1.9. このような事実の証明は、図式を描いて与えることもできる。

$$\begin{array}{ccccc} S \times S & \overset{f \times f}{\to} & T \times T & \overset{g \times g}{\to} & U \times U \\ \downarrow \circ_S & \circlearrowright & \downarrow \circ_T & \circlearrowright & \downarrow \circ_U \\ S & \overset{f}{\to} & T & \overset{g}{\to} & U \end{array}$$

を見る。左上の元を下右右 ($\circ_s, f, g$ の順にすすむ) と写したものと、右下右（$f \times f, \circ_T, g$ の順に進む）と写したものは同じものである（左側の正方形の可換性）。次に、この右下右と写したものは、右右下（$f \times f, g \times g, \circ_U$ と進む）と移したものは同じものである（右側の正方形の可換性）。よって、全体の長方形は可換である。上の辺二つの合成は

$$(g \times g) \circ (f \times f) = (g \circ f) \times (g \circ f)$$

であるから、全体の長方形の可換性は

$$\begin{array}{ccc} S \times S & \overset{(g \circ f) \times (g \circ f)}{\to} & U \times U \\ \downarrow \circ_S & \circlearrowright & \downarrow \circ_U \\ S & \overset{g \circ f}{\to} & U \end{array}$$

の可換性を意味する。この図式の可換性は、$g \circ f$ のマグマ準同型性に他ならない。定義 2.1.7 参照。

定義 2.1.10. $(S, \circ_S)$ をマグマとする。恒等写像

$$\mathrm{id}_S : S \to S$$

はマグマ準同型である。このマグマ準同型を S 上の**恒等射** (identity morphism) と呼ぶ。

$(T, \circ_T)$ もマグマとする。マグマ準同型 $f : S \to T$ と $g : T \to S$ であって

$$g \circ f = \mathrm{id}_S, \quad f \circ g = \mathrm{id}_T$$

となるものがあるとき、g を f の**逆射** (inverse morphism)、f を g の逆射という。逆射 を持つような準同型を**可逆射** (invertible morphism)、または **同型射** (isomorphism)、**同型写像**、または単に**同型**という。 $(S, \circ_S)$ と $(T, \circ_T)$ の間に同型写像があるとき、これらのマグマは**同型** (isomorphic) であるという。

定理 1.1.25 により、同型写像は全単射である。同型写像は S の元と T の元の一対一対応であって、演算の構造を保つ (注 2.1.5) ものを与えている。

例 2.1.11. 正の実数の集合を $\mathbb{R}_{>0}$ と記す。指数関数 exp を

$$\exp : \mathbb{R} \to \mathbb{R}_{>0}, \quad x \mapsto e^x$$

で定義する ($e = 2.718\cdots$) と、これは log ($= \log_e$) を逆写像とする全単射である。

exp は、$(\mathbb{R}, +)$ から $(\mathbb{R}_{>0}, \times)$ へのマグマ準同型写像である。任意の 2 実数 x, x' に対し

$$e^{x+x'} = e^x \times e^{x'}$$

が成り立つからである。

log は $(\mathbb{R}_{>0}, \times)$ から $(\mathbb{R}, +)$ へのマグマ準同型である。任意の正の二実数 x, x' に対し

$$\log(x \times x') = \log x + \log x'$$

が成り立つからである。

よって、exp はマグマ同型写像であり、log はその逆射である。(注 : ここで、e を 1 でない任意の正の実数 a に置き換え、a を底とする指数関数 a^x, 対数関数 $\log_a$ を考えても、マグマ同型が得られる。この性質については、e が特別なわけではない。)

注意 2.1.12. いちいち「$(S, \circ)$ をマグマとする」と書くのは長い。ので、しばしば、次のような端折った言い方をする。「$f : S \to T$ をマグマ準同型とする」と言ったら、それだけで「S にはマグマの構造が与えられており、T にもマグマの構造が与えられており、f はマグマ準同型である」ということを意味していることにする。

例えば、命題 2.1.8 は

「$f : S \to T, g : T \to U$ をマグマ準同型とすると、その合成 $g \circ f$ もマグマ準同型である。」

と短く言える。

命題 2.1.13. $f : S \to T$ がマグマ準同型でかつ全単射であるとする。このとき、f の逆写像 g がただ一つ存在する。$g : T \to S$ はマグマ準同型となり、したがって f の逆射となる。

証明. 定理 1.1.25 により、逆写像 g が存在し、系 1.1.24 により、それはただ一つである。この g が、マグマ準同型であることを言えばよい。それには、任意の $t, t' \in T$ に対し

$$g(t \circ_T t') = g(t) \circ_S g(t')$$

が成り立つことを言えばよい。

さて、f は単射であるから、上の等式を確かめるには f で送った像をみて

$$f(g(t \circ_T t')) = f(g(t) \circ_S g(t'))$$

を確かめれば十分である (f が単射なら、$f(x) = f(x') \Rightarrow x = x'$)。しかるに、$f \circ g = \mathrm{id}_T$ であるから、左辺は $t \circ_T t'$ と等しく、右辺は f が準同型であることを使うと $f(g(t)) \circ_T f(g(t'))$ となり、$t \circ_T t'$ に一致する。 □

問題 2.3. $\exp : \mathbb{R} \to \mathbb{R}_{>0}$ が $(\mathbb{R}, +)$ から $(\mathbb{R}_{>0}, \times)$ へのマグマ準同型であることだけを使って、その逆写像 $\log$ が $x, x' > 0$ に対し

$$\log(x \times x') = \log(x) + \log(x')$$

を満たすことを示せ。

命題 2.1.14. $(S, \times)$ をマグマとし、T を集合とする。$f, g \in \mathrm{Map}(T, S)$ に対して

$$f \tilde{\times} g \in \mathrm{Map}(T, S), \quad (f \tilde{\times} g)(t) := f(t) \times g(t)$$

と定義すると $(\mathrm{Map}(T, S), \tilde{\times})$ はマグマである。すなわち、「マグマを値域とする関数の集合は自然にマグマ」となる。

問題 2.4. 上の命題を示せ。

注意 2.1.15. 微分積分学で習う実数上の実関数全体は $\mathrm{Map}(\mathbb{R}, \mathbb{R})$ である。$(\mathbb{R}, +)$ はマグマなので、実関数全体にも和 $\tilde{+}$ が定義される。これは、通常言うところの「関数の和」である。

実際、$f, g \in \mathrm{Map}(\mathbb{R}, \mathbb{R})$ に対してそれらの関数としての和 $f+g \in \mathrm{Map}(\mathbb{R}, \mathbb{R})$ は、$(f+g)(x) := f(x) + g(x)$ で定義される。

2.1.2　部分マグマ

定義 2.1.16. $(S, \circ)$ をマグマとする。$T \subset S$ を部分集合とする。二項演算 $\circ$ を T に制限すると

$$\circ : T \times T \to S$$

を得る。($\circ$ という同じ記号を使った。厳密には $\circ|_{T \times T}$ と書くべきである。ここで、この縦線 $|$ は「写像 $\circ$ の定義域を $T \times T$ に制限する」ことを意味する。) 写像 $\circ$ による $T \times T$ の像が T に入るとき、$\circ$ は

$$\circ' : T \times T \to T$$

を定め、したがって $(T, \circ')$ はマグマとなる。これを $(S, \circ)$ の**部分マグマ** (sub magma) という。$\circ'$ のことを、$\circ|_T$ または（混乱を招かないときは通常）$\circ$ と記す。

つまり、$T \subset S$ が演算 $\circ$ に閉じている (注 1.2.3 参照、S, T が逆であることに注意) とき、$\circ$ を T に制限して得られるマグマを部分マグマというのである。

問題 2.5. 次を証明せよ。

1. $(\mathbb{N}, +)$ は $(\mathbb{Z}, +)$ の、$(\mathbb{Z}, +)$ は $(\mathbb{Q}, +)$ の部分マグマである。
2. 実数から実数への関数 $\mathrm{Map}(\mathbb{R}, \mathbb{R})$ は和に関してマグマとなる。実数から実数への連続関数全体は、その部分マグマとなる。(連続関数の和は連続関数だから。)

定義 2.1.17. S を集合とし、$T \subset S$ とする。このとき、$t \in T$ を $t \in S$ に写す写像を**埋め込み** (immersion, embedding) といい、

$$\iota : T \hookrightarrow S$$

であらわす。(なお、ι はイオタと読み、ギリシャ語の i である。)

命題 2.1.18. $(S, \circ)$ をマグマとし、$T \subset S$ とする。$\iota : T \hookrightarrow S$ が準同型になるようなマグマの構造 $\circ_T$ が T に入る必要十分条件は、T が $\circ$ に閉じていることである。このとき、$\circ_T$ は $\circ$ の $T \times T$ への制限となり、したがってただ一つ存在する。

定義 2.1.19. 上のように埋め込み ι が $(T, \circ_T)$ から $(S, \circ)$ への準同型となるとき、ι を**マグマの埋め込み** (immersion of magma, embedding of magma) といい、

$$\iota : T \hookrightarrow S$$

であらわす。(T, S がマグマのときにこう書いたら、ι は準同型であることも意味している。)

問題 2.6. 命題 2.1.18 を示せ。

2.1.3 商マグマ

定理 2.1.20. $(S, \circ)$ をマグマとし、$\sim$ を S 上の同値関係とする。商写像

$$q : S \to S/\sim$$

がマグマ準同型となるような二項演算 $\bar{\circ}$ が $S/\sim$ に定義される必要十分条件は、$\circ$ と $\sim$ がコンパチブルである (系 1.3.23 参照) ことである。このとき、$\bar{\circ}$ はただ一通りに定まる。$(S/\sim, \bar{\circ})$ を S の $\sim$ による**商マグマ**といい、q を**商準同型**と言う。

証明. これは、系 1.3.23 に他ならない。 □

例 2.1.21. 問題 1.19 が言っているのは、マグマ $(\mathbb{Z} \times \mathbb{N}, \tilde{+})$ に対し、$((\mathbb{Z} \times \mathbb{N})/\sim, +)$ はその商マグマであるということである。

問題 2.7. $(\mathbb{Z}, \times)$ に対し、$(\mathbb{Z}/m, \bar{\times})$ はその商マグマとなることを示せ。

定理 2.1.22. $(X, \circ_X)$ をマグマとし、$\sim$ を X 上の $\circ_X$ とコンパチブル (系 1.3.23 の意味で) な同値関係とする。$(X/\sim, \bar{\circ})$ で商マグマを表す。$q : X \to X/\sim$ を商準同型とし、任意のマグマ $(Y, \circ_Y)$ と任意のマグマ準同型 $f : X \to Y$ を考える。

f が $\sim_X$ とコンパチブルである（定理 1.3.20 の意味で）、すなわち任意の $x, x' \in X$ に対し

$$x \sim_X x' \Rightarrow f(x) = f(x')$$

が成立しているならば、定理 1.3.20 により写像 $\bar{f} : X/\sim_X \to Y$ であって、

$$f = \bar{f} \circ q$$

なる性質をもつものが唯一つ存在する。このとき、$\bar{f}$ はマグマ準同型になる。

この状況を、マグマ準同型 f は同値関係 $\sim_X$ にコンパチブルであるといい、また $\bar{f}$ が well-defined であるという。

証明. 定理 1.3.20 により写像として与えられた $\bar{f}$ がマグマ準同型になることさえ言えばよい。が、

$$\bar{f}([x]\bar{\circ}[x']) = \bar{f}([x \circ_X x']) = f(x \circ_X x') = f(x) \circ_Y f(x') = \bar{f}([x]) \circ_Y \bar{f}([x'])$$

より言えた。 □

定理 2.1.23. (マグマの準同型定理) $(X, \circ_X)$、$(Y, \circ_Y)$ をマグマとし、$f : X \to Y$ なるマグマ準同型が与えられたとする。$f(X) \subset Y$ で f による X の像を表す。このとき、

1. $f(X)$ は Y の部分マグマである。
2. $\sim_f$ は $\circ$ とコンパチブルな同値関係である。したがって、$X/\sim_f$ は商マグマとなる。
3. f が
$$X \xrightarrow{q} X/\sim_f \xrightarrow{\bar{f}} Y$$
なる合成となるような写像 $\bar{f}$、すなわち
$$f = \bar{f} \circ q$$
なる $\bar{f}$ がただ一つ存在するが、これはマグマ準同型となる。そして、$\bar{f}$ の終集合を $f(X)$ に制限して得られる
$$\bar{f} : X/\sim_f \to f(X)$$
はマグマ同型となる。

証明.

1. 像 $f(X)$ の任意の二元は $f(x), f(x')$ とあらわせる。f の準同型性より $f(x) \circ_Y f(x') = f(x \circ_X x') \in f(X)$ であるから、$f(X) \subset Y$ は $\circ_Y$ に閉じている。
2. $x_1 \sim_f x_1', x_2 \sim_f x_2'$ ならば $f(x_1) = f(x_1'), f(x_2) = f(x_2')$。$f$ の準同型性を二度使うと
$$f(x_1 \circ_X x_2) = f(x_1) \circ_Y f(x_2) = f(x_1') \circ_Y f(x_2') = f(x_1' \circ_X x_2')$$
となる。両端を比べて $x_1 \circ x_2 \sim_f x_1' \circ x_2'$。

3. 集合の準同型定理 1.3.33 から $f = \bar{f} \circ q$ を満たす

$$\bar{f} : X/\sim_f \to f(X)$$

が唯一つ存在する。「$x \sim_f x'$ ならば $\sim_f$ の定義により $f(x) = f(x')$」であるから、定理 2.1.22 の条件を満たし $\bar{f}$ はマグマ準同型である。$\bar{f}$ が全単射であることは、集合の準同型定理 1.3.33 からしたがう。すると、$\bar{f}$ は準同型でかつ全単射であるから命題 2.1.13 より同型となる。

□

問題 2.8.

1.
$$T = \{z \in \mathbb{C} | |z| = 1\}$$
とおく。$\times$ を複素数の積とすると、$(\mathbb{C}, \times)$ はマグマである。$T \subset \mathbb{C}$ はその部分マグマであることを示せ。

2.
$$\mathrm{Exp} : (\mathbb{R}, +) \to (\mathbb{C}, \times), \quad x \mapsto e^{2\pi i x}$$
はマグマ準同型であることを示せ。

3. マグマ同型
$$(\mathbb{R}/\equiv, +) \cong (T, \times)$$
を示せ。ここに $\equiv$ は、
$$x \equiv x' \Leftrightarrow x - x' \in \mathbb{Z}$$
で定義される $\mathbb{R}$ 上の同値関係である。

2.2 半群

2.2.1 結合法則と半群

定義 2.2.1. **半群** (semigroup)G とは、材料として

GA 集合 G_0 (**台集合**などと呼ばれる)

GB G_0 上の二項演算 $\circ$(積、合成などと呼ばれる)

が与えられて、次の性質 (**半群の公理**、axiom of semigroups と呼ばれる) を満たすもの。

G1 (**結合法則**, associative law)

$$g_1, g_2, g_3 \in G_0 \Rightarrow (g_1 \circ g_2) \circ g_3 = g_1 \circ (g_2 \circ g_3).$$

(注 上の表記では「任意の $g_1, g_2, g_3 \in G_0$ に対して上の等式が成り立つ」ことを意味している。「任意の」という言葉を省略していることになる。以下でも、「公理」においては「任意の」という言葉を省略することにする。多くの教科書で断りなくこのような省略が行われている。)

このように、「半群 G」といったら「$(G_0, \circ)$ の組であって二項演算 $\circ$ が結合法則を満たすもの」のことである。この意味で $G = (G_0, \circ)$ と書くこともある。が、通常しばしば、台集合 G_0 のことも簡便のために G と書いてしまうことが多い。これはあくまで慣習的な記法であるが、標準的である。したがって、半群 $G = (G_0, \circ)$ において、$g \in G_0$ を単に $g \in G$ と書き、写像 $f : G_0 \to S$ は $f : G \to S$ と書く。(注意 : 同じコメントが、マグマについても言える。すなわち、マグマ G と言えば $G = (G_0, \circ)$ なる、集合と二項演算の組であり、G_0 を G の台集合という。)

例 2.2.2. 1. $(\mathbb{Z}, +)$, $(\mathbb{N}, +)$, (n 次正方行列の集合, 行列の積) は半群である。

2. $(\mathbb{Z}, -)$ は半群でない。一般には

$$(a - b) - c \neq a - (b - c)$$

だからである。

3. $(\mathbb{N}, \text{ベキ})$ は半群でない。

$$2^{(1^2)} \neq (2^1)^2$$

だから。

4. S を集合とする。S からそれ自身への写像の集合と、写像の合成の組

$$(\mathrm{Map}(S, S), \circ)$$

は半群である。1.1.3 節の式 (1.2) より従う。

結合法則はなぜ現れて、なぜ重要なのか？著者にもよくわからない。が、例えば写像の合成をはじめ、結合法則を満たす演算はたくさんある。また、次の問題は、「結合法則と、ある写像がマグマの準同型であることとが同値」であることを示している。

問題 2.9. $(S, \cdot)$ をマグマとする。定理 1.1.30 により、二項演算

$$\cdot : S \times S \to S$$

は

$$L : S \to \mathrm{Map}(S, S)$$

と対応している。ここに、$L(s)$ は左 (left) から s を $\cdot$ する写像

$$L(s) : t \to s \cdot t$$

である。(左からの積、left multiplication という。) L が $(S, \cdot)$ から $(\mathrm{Map}(S, S), \circ)$ へのマグマ準同型であることと、$\cdot$ が結合法則を満たすこととが同値であることを示せ。

ヒント：マグマ準同型であることは、

$$\forall s, s' \in S \quad L(s \cdot s') = L(s) \circ L(s')$$

と言い換えられる。この両辺に $s'' \in S$ を食べさせると、結合法則が得られる。

2.2.2 半群の準同型

定義 2.2.3. 半群 $G = (G_0, \circ)$ から半群 $G' = (G'_0, \circ')$ への**半群準同型** (homomorphism of semigroups) とは、台集合の間の写像 $f : G_0 \to G'_0$ であって、

$$\forall s_1, s_2 \in G_0 \qquad f(s_1 \circ s_2) = f(s_1) \circ' f(s_2)$$

が成立するものをいう。

すなわち、半群の間の準同型とは、それらの半群をマグマとみなしたときのマグマ準同型である。では、半群を定義する公理 [G1] は無視していいのか？いいのである。以下、モノイドや群や環や体の準同型の定義でも同様であるが、準同型に要請されるのは演算とのコンパチビリティだけであり、公理は無視される。「それはなぜか」、と聞かれると、筆者にはよくわからない。準同型の定義において公理を無視しないような数学もあるかも知れない。

命題 2.2.4. 半群 G, G', G'' とそれらの間の準同型 $f : G \to G', g : G' \to G''$ があるとき、それらの合成 $g \circ f : G \to G''$ も準同型である。

証明. 半群の準同型とはマグマの準同型のことだから、命題 2.1.8 より直ちに従う。 □

これは「二つの準同型の合成は準同型」という形の命題である。以下、モノイド、群、環、体、いずれにおいても「二つの準同型の合成は準同型」という命題が示される。

マグマの場合の定義 2.1.10 と完全に同じように、次のような定義をする。(実際、「マグマ」という単語を全て「半群」と書き換えただけである。)

定義 2.2.5. $(S, \circ_S)$ を半群とする。恒等写像

$$\mathrm{id}_S : S \to S$$

は半群準同型である。この半群準同型を S 上の恒等射 (identity morphism) と呼ぶ。

$(T, \circ_T)$ も半群とする。半群準同型 $f : S \to T$ と $g : T \to S$ であって

$$g \circ f = \mathrm{id}_S, \quad f \circ g = \mathrm{id}_T$$

となるものがあるとき、g を f の、f を g の逆射という。逆射を持つような準同型を可逆射、または同型射、同型写像、または単に同型という。

$(S, \circ_S)$ と $(T, \circ_T)$ の間に同型写像があるとき、**これらの半群は同型である**という。

命題 2.2.6. $f : S \to T$ が半群準同型でかつ全単射であるとする。このとき、f の逆写像 g が存在し、$g : T \to S$ も半群準同型となり、したがって f の逆射となる。

証明. 半群準同型とは「半群から半群への」マグマ準同型のことであるから、命題 2.1.13 から直ちに従う。 □

このように、「準同型でかつ全単射ならば同型」という命題は、モノイド・群・環・体の全てで成り立つ。これは代数系に特有の現象である。「位相空間」の概念を御存じの読者は、「X, Y が位相空間で $f : X \to Y$ が連続な全単射とする。このとき、f^{-1} は連続とはかぎらない。よって、f は同相写像とは限らない」という現象を御存じと思う。たとえば、$X = Y = \mathbb{R}$ とし、X に離散位相を入れて Y に通常の実数の位相を入れると $\mathrm{id}_{\mathbb{R}} : \mathbb{R} \to \mathbb{R}$ は連続な全単射だが、その逆写像は連続にならない。(この位相についての注意書きが理解できなくても、本書を読むには全く影響しないのでご心配なく。)

定義 2.2.7.　1. S, S' をマグマとする。S から S' へのマグマ準同型の集合を

$$\mathrm{Hom}_{\mathrm{magma}}(S, S')$$

で表す。特に、$S = S'$ のとき

$$\mathrm{End}_{\mathrm{magma}}(S) := \mathrm{Hom}_{\mathrm{magma}}(S, S)$$

とおいて S のマグマ自己準同型 (magma endomorphism) の集合という。

2. S, S' を半群とする。S から S' への半群準同型 (semigroup homomorphism) の集合を

$$\mathrm{Hom}_{\mathrm{semigp}}(S, S')$$

で表す。特に、$S = S'$ のとき

$$\mathrm{End}_{\mathrm{semigp}}(S) := \mathrm{Hom}_{\mathrm{semigp}}(S, S)$$

とおいて S の半群自己準同型 (semigroup endomorphism) の集合という。

以下でみるように、自己準同型の集合は写像の合成に関して半群（さらにモノイド）である。

2.2.3　部分半群

定義 2.2.8. (部分半群, sub-semigroup)　半群 $G = (G_0, \circ)$ の部分半群とは、G_0 の部分集合 S であって、S が $\circ$ について閉じていて半群となっているものを言う。

命題 2.2.9. 上で、$S \subset G_0$ が部分半群となる必要十分条件は S が $\circ$ に閉じていることである。

証明. 定義より、$\circ$ について閉じていることは必要である。十分性を示す。閉じていると仮定して、部分半群になることを示せばよい。閉じているのだから、$\circ$ は制限により S における二項演算を定める。これが結合法則を満たせばよいが、それには

$$a \circ (b \circ c) = (a \circ b) \circ c$$

が任意の S の元について成り立つことを示せばよい。しかし、G_0 が半群であることからこれは任意の G_0 の元について成り立つのであり、したがって $S \subset G_0$ の元についても成り立つ。 □

すなわち、半群 G の部分半群とは、G をマグマとみなしたときの部分マグマと一致する。ここでも公理 [G1] は自動的に成立してしまう。

例 2.2.10. 例 2.2.2 で見たとおり、集合 S に対し S からそれ自身への写像の全体 $\mathrm{Map}(S, S)$ は写像の合成 $\circ$ について半群となる。

1. $\mathrm{Map}(\mathbb{R}, \mathbb{R})$ の中で、連続写像となるものの全体を C とする。C は $(\mathrm{Map}(\mathbb{R}, \mathbb{R}), \circ)$ の部分半群である。C が合成について閉じているということは、「連続関数の合成は連続関数である」という、よく知られた事実と同値である。
2. S をマグマとする。$(\mathrm{End}_{\mathrm{magma}}(S), \circ)$ は $(\mathrm{Map}(S, S), \circ)$ の部分半群である。
3. S を半群とする。$(\mathrm{End}_{\mathrm{semigp}}(S), \circ)$ は $(\mathrm{Map}(S, S), \circ)$ の部分半群である。

問題 2.10. 上の例において、部分半群であることをそれぞれ証明せよ。

2.2.4 商半群

半群に、二項演算とコンパチブルな同値関係があるとき、商集合は自動的に半群となる。これを商半群 (quotient semigroup) という。 マグマの場合の定理 2.1.20 参照。

定理 2.2.11. $(S, \circ)$ を半群とし、$\sim$ を S 上の同値関係とする。商写像

$$q : S \to S/\sim$$

が半群準同型となるような二項演算 $\bar{\circ}$ が $S/\sim$ に定義される必要十分条件は、$\circ$ と $\sim$ がコンパチブルである (系 1.3.23 参照) ことである。

このとき、$\bar{\circ}$ はただ一通りに定まる。$(S/\sim, \bar{\circ})$ を S の $\sim$ による商半群といい、q を商準同型と言う。

証明. 今、q が半群準同型となるような $\bar{\circ}$ が定義できたとすると、マグマの場合の定理 2.1.20 により $\circ$ と $\sim$ はコンパチブルでなければならない。

逆に、$\circ$ と $\sim$ がコンパチブルであったとき、q が半群準同型となるような $\bar{\circ}$ が定義できることを言う。コンパチブルを仮定する。マグマの場合の定理 2.1.20 により q がマグマ準同型となるような $\bar{\circ}$ は定義できる。これが結合法則 [G1] を満たすことを示せばよい。$S/\sim$ の任意の元は $[g]$ $(g \in S)$ の形に書けるから、

$$([g_1]\bar{\circ}[g_2])\bar{\circ}[g_3] = [g_1]\bar{\circ}([g_2]\bar{\circ}[g_3])$$

を示せばよいのであるが、これは $(S, \circ)$ が半群であるゆえ

$$(g_1 \circ g_2) \circ g_3 = g_1 \circ (g_2 \circ g_3)$$

を満たすので、両辺に [] をほどこし、「$q = [] : S \to S/\sim$ がマグマの準同型である」こと、すなわち

$$[g_1 \circ g_2] = [g_1]\bar{\circ}[g_2]$$

であることを繰り返し使えば示せる。 □

ここでも、$(S/\sim, \bar{\circ})$ の結合法則 [G1] は自動的に従う。

2.2.5 準同型定理

定理 2.2.12. $(X, \circ_X)$ を半群とし、$\sim$ を X 上の $\circ_X$ とコンパチブル (系 1.3.23 参照) な同値関係とする。$(X/\sim, \bar{\circ})$ で商半群を表す。$q : X \to X/\sim$ を商準同型とし、任意の半群 $(Y, \circ_Y)$ と任意の半群準同型 $f : X \to Y$ を考える。

$\sim_X$ と f がコンパチブル、すなわち任意の $x, x' \in X$ に対し

$$x \sim_X x' \Rightarrow f(x) = f(x')$$

となるとすると、定理 1.3.20 により写像 $\bar{f} : X/\sim_X \to Y$ であって、

$$f = \bar{f} \circ q$$

なる性質をもつものが唯一つ存在する。このとき、$\bar{f}$ は半群準同型である。

この状況を、半群準同型 f は同値関係 $\sim_X$ とコンパチブルであるといい、また $\bar{f}$ が well-defined であるという。

証明. 定理 2.1.22 と比べると、「マグマ準同型 $\bar{f}$ が半群準同型であること」を示せばよいが、これは「半群間のマグマ準同型は半群準同型であること」から明らか。 □

定理 2.2.13. (半群の準同型定理)
$(X, \circ_X)$、$(Y, \circ_Y)$ を半群とし、$f : X \to Y$ なる半群準同型が与えられたとする。$f(X) \subset Y$ で f による X の像を表す。このとき、

1. $f(X)$ は Y の部分半群である。
2. $\sim_f$ は $\circ$ とコンパチブルな同値関係である（系 1.3.23 の意味で）。したがって、$X/\sim_f$ は商半群である。
3. f が
$$X \xrightarrow{q} X/\sim_f \xrightarrow{\bar{f}} Y$$
なる合成となるような $\bar{f}$、すなわち
$$f = \bar{f} \circ q$$
なる $\bar{f}$ がただ一つ存在するが、これは半群準同型である。そして、その終集合を $f(X)$ に制限して得られる
$$\bar{f} : X/\sim_f \to f(X)$$
は半群同型となる。

つまり、定理 2.1.23 は半群に対してもそのまま成り立つ。

証明. 定理 2.1.23 に現れるマグマ準同型、マグマ同型、商マグマ、部分マグマという 4 つの概念が、それぞれ「登場するマグマが全て半群である」場合、自動的に半群準同型、半群同型、商半群、部分半群となることから従う。 □

2.2.6　自然数と指数法則

半群においては、結合法則により

$$(g_1 \circ g_2) \circ ((g_3 \circ g_4) \circ g_5) = ((g_1 \circ g_2) \circ (g_3 \circ g_4)) \circ g_5 = (((g_1 \circ g_2) \circ g_3) \circ g_4) \circ g_5$$

である。一般に、n 個の元の積をとったとき、かっこのつけかたによらず結果は同じとなる。(厳密には証明が必要である。) そこで、上のような積を単に

$$g_1 \circ g_2 \circ g_3 \circ g_4 \circ g_5$$

と記述する。特に、n が自然数のとき

$$g \circ g \circ g \circ \cdots \circ g \quad (n \text{ 個})$$

を g^n と記す。

定理 2.2.14. (半群における**指数法則**)
$(G_0, \circ)$ を半群とし、$g \in G_0$ を一つの元とする。自然数 n, m に対し次が成立する。

$$(g^n) \circ (g^m) = g^{n+m}$$

問題 2.11. 上の定理を証明せよ。一般のマグマに対しては、どのような障害が生じるか考察せよ。

系 2.2.15. $(G_0, \circ)$ を半群とし、$g \in G_0$ を一つの元とする。このとき、

$$f : (\mathbb{N}, +) \to (G_0, \circ)$$

なる半群準同型であって、$1_{\mathbb{N}} \mapsto g$ となるものが唯一つ存在する。

証明. もし存在したとすると、

$$\begin{aligned} f(2) &= f(1+1) = f(1) \circ f(1) = g \circ g = g^2 \\ f(3) &= f(1+2) = f(1) \circ f(2) = g \circ (g \circ g) = g^3 \\ &\cdots \end{aligned}$$

により、

$$f(n) = g^n$$

となる。これで一意性が言えた。f が半群準同型になるということを数式で書くと、$f(n+m) = f(n) \circ f(m)$、言い換えれば $g^{n+m} = g^n \circ g^m$ である。これは上記の指数法則そのものである。 □

2.3 モノイド

2.3.1 単位元とモノイド

定義 2.3.1. $(S, \circ)$ をマグマとする。このマグマの**左単位元** (left unit) とは、S の元 a であって、

$$\forall s \in S \quad a \circ s = s$$

を満たすものであり、**右単位元** (right unit) とは S の元 b であって、

$$\forall s \in S \quad s \circ b = s$$

を満たすものである。
右単位元でかつ左単位元でもある元を単に**単位元** (unit) という。

問題 2.12. もしマグマに左単位元と右単位元が存在すれば、それらは一致することを示せ。(特に、単位元は左単位元でかつ右単位元であるから、マグマに単位元があればそれはただ一つである。)

ヒントは、上の定義で言えば $a \circ b$ を計算してみることである。

定義 2.3.2. 単位元をもつ半群を**モノイド** (monoid、単位的半群) という。 すなわち、モノイド G とは材料としては

GA 集合 G_0(台集合などと呼ばれる)

GB G_0 上の二項演算 $\circ$(積、合成などと呼ばれる)

GC $e \in G_0$(単位元と呼ばれる)

の組 $(G_0, \circ, e)$ であって、次の性質 (モノイドの公理と呼ばれる) を満たすもの。

G1 (結合法則, associative law)

$$\forall g_1, g_2, g_3 \in G_0 \quad (g_1 \circ g_2) \circ g_3 = g_1 \circ (g_2 \circ g_3).$$

G2 (**単位法則**, unit law)

$$\forall g \in G_0 \quad g \circ e = g, e \circ g = g.$$

注意 2.3.3. この定義にあるように、モノイドとは $(G_0, \circ, e)$ の組のことである。が、しばしば「$(G_0, \circ)$ はモノイドである」という言い方をする。これは、上の問題 2.12 により、単位元は存在すれば一意的に決まってしまうからである。「モノイドであれば定義から単位元があり、それはただ一つに定まるので、単位元を指定する必要はない」という考え方である。別の観点からすると、モノイドの定義を「単位元を持つ半群を、モノイドという」としても同値である。

一方、次の節 2.3.2 で説明するように、「モノイド準同型」の定義では「単位元を単位元に写す」という条件を課す。単位元を「モノイドの材料（0 項演算）」とみなす方が、より自然で現代的である。

例 2.3.4.

1. $(\mathbb{N}, \times, 1)$ はモノイドである。
2. 半群 $(\mathbb{N}, +)$ はモノイドにならない。和に関する単位元が $\mathbb{N}$ にないからである。
3. 0 を付け加えて、$(\mathbb{N} \cup \{0\}, +, 0)$ とするとこれはモノイド。
4. 0 以上の有理数の集合は、和に関してモノイドとなる。
5. $(\mathrm{Map}(S, S), \circ, \mathrm{id}_S)$ はモノイドである。ここに、$\circ$ は写像の合成をあらわす。

2.3.2　モノイド準同型

定義 2.3.5. $(S, \circ_S, e_S)$, $(T, \circ_T, e_T)$ をモノイドとする。S から T への**モノイド準同型** (monoid homomorphism) とは、$f : S \to T$ なる写像であって、マグマ準同型でかつ単位元を単位元に写すもの。すなわち、

HB $\forall s, s' \in S, \quad f(s \circ_S s') = f(s) \circ_T f(s')$

HC $f(e_S) = e_T$

の二つをみたすもの。

例 2.3.6. 先に見た

$$\exp : (\mathbb{R}, +, 0) \to (\mathbb{R}, \times, 1)$$

はモノイド準同型である。マグマ準同型であり、かつ単位元 0 は $e^0 = 1$ に移されるからである。

いままで見た半群準同型の多くがモノイド準同型ともなっている。

上の定義で、[HB] は [GB] に、[HC] は [GC] に対応している。1.2.1 節の用語を使えば、[GB] は「集合に二項演算が与えられている」ということができるし、[GC] は「集合に 0 項演算が与えられている」ということができる。

[HB] は定義 2.1.7 で見たように次の可換図式で表すことができる。

$$\begin{array}{ccc} S \times S & \stackrel{f \times f}{\to} & T \times T \\ \downarrow \circ_S & \circlearrowright & \downarrow \circ_T \\ S & \stackrel{f}{\to} & T \end{array}$$

同じように、少し無理をすれば [HC] は次の可換図式により記述される。

$$\begin{array}{ccc} S^0 & \stackrel{f^0}{\to} & T^0 \\ \downarrow e_S & \circlearrowright & \downarrow e_T \\ S & \stackrel{f}{\to} & T \end{array}$$

上の行は一元集合から一元集合への唯一つ存在する写像

$$S^0 = \{()\} \to T^0 = \{()\}, \quad () \mapsto ()$$

であり、左縦の写像は元「()」を e_S に移す写像、同様に右縦の写像は () を e_T に移す写像である。左上の () を、左下経由で右下に持っていくと $f(e_S)$ であり、右上経由で持っていくと e_T となる。したがって図式の可換性は、

$$f(e_S) = e_T$$

と同値である。こうして、「モノイド準同型の公理 [HB] は二項演算 $\circ$ を保つこと、公理 [HC] は 0 項演算 e を保つこと」(次節参照) と言い換えることができる。一般に、代数構造の間の準同型の定義は、「指定された演算を全て保つ写像」として与えられる。モノイドの場合は $\circ$ と e が指定された演算である。

2.3.3 写像が演算を保つこと

二項演算を n 項演算に一般化して、次のように「**写像が演算を保つ**（保存する）こと」(mapping preserves operation) を定義する。

定義 2.3.7. S を n 項演算 $\alpha_S : S^n \to S$ の与えられている集合、T を n 項演算 $\alpha_T : T^n \to T$ の与えられている集合とする。写像 $f : S \to T$ が α_S, α_T を**保つ**とは、

$$\forall s_1, s_2, \ldots, s_n \quad f(\alpha_S(s_1, s_2, \ldots, s_n) = \alpha_T(f(s_1), f(s_2), \ldots, f(s_n))$$

が成立すること。添え字を落として「f は α を保つ」ということが多い。

この定義は、図式

$$\begin{array}{ccc} S^n & \stackrel{f^n}{\to} & T^n \\ \downarrow \alpha_S & & \downarrow \alpha_T \\ S & \stackrel{f}{\to} & T \end{array}$$

が可換であるとも言い換えられる。ここに上の行の $f^n : S^n \to T^n$ は、

$$f^n(s_1, \ldots, s_n) = (f(s_1), \ldots, f(s_n))$$

で定義される。

この用語を使うならば、「マグマ準同型とは、台集合の間の写像であって、指定された二項演算 $\circ$ を保つもの」と言い換えられるし、「モノイド準同型とは、台集合の間の写像であって、指定された二項演算 $\circ$ ならびに指定された 0 項演算 e を保つもの」と言い換えられる。

後の節で扱う「群」でも「環」でもそうだが、「準同型」を定義するときに写像に要請される条件は、「指定された演算を保つこと」のみであり、公理は構わなくて良い。

注意 2.3.8. 写像 f に対し、f^n という記法には二つの違った意味がありうる。上の場合には $f : S \to T$ で

$$f^n : S^n \to T^n$$

であるが、一方 $f \in \mathrm{Map}(S, S)$ のときには関数の合成

$$f^n := f \circ f \circ \cdots \circ f \in \mathrm{Map}(S, S)$$

をあらわしている可能性がある。(定理 2.2.14 参照。) 文脈に従って、どちらのことなのかを各自判断して欲しい。

命題 2.3.9. (S, α_S), (T, α_T), (U, α_U) を、それぞれ集合と n 項演算の組とする。$f : S \to T$ が α_S, α_T を保ち、$g : T \to U$ が α_T, α_U を保つならば、

$$g \circ f : S \to U$$

は α_S, α_U を保つ。

証明は機械的である。次の図式を使うこともできる。

$$\begin{array}{ccccc} S^n & \xrightarrow{f^n} & T^n & \xrightarrow{g^n} & U^n \\ \downarrow \alpha_S & \circlearrowright & \downarrow \alpha_T & \circlearrowright & \downarrow \alpha_U \\ S & \xrightarrow{f} & T & \xrightarrow{g} & U \end{array}$$

注意 2.1.9 参照のこと。

問題 2.13. 上の命題 2.3.9 を証明せよ。

系 2.3.10. 二つのモノイド準同型の合成は、モノイド準同型である。

証明. 証明するべきことは $g \circ f$ が二項演算 $\circ$ ならびに 0 項演算 e を保つことである。が、命題 2.3.9 からどちらも従う。なお、系としてではなく、直接証明することも易しい。命題 2.1.8 により、$\circ$ が保たれていることがわかる。e については、$f(e_S) = e_T$(f の準同型性から従う) の両辺の g による像をとると $g(f(e_S)) = g(e_T) = e_U$ である。ここで、二番目の等号に、g の準同型性を用いた。 □

次は、二項演算に関する系 1.3.23 の一般化である。

定理 2.3.11. S を n 項演算 $\alpha : S^n \to S$ の与えられている集合とし、$\sim$ を α とコンパチブルな S 上の同値関係、すなわち任意の $s_1, s_1', \ldots, s_n, s_n' \in S$ に対し

$$s_1 \sim s_1', s_2 \sim s_2', \ldots s_n \sim s_n' \Rightarrow \alpha(s_1, \ldots, s_n) \sim \alpha(s_1', \ldots, s_n')$$

とする。このとき、商集合 $S/\sim$ には n 項演算 $\bar{\alpha}$ であって

$$\bar{\alpha}([s_1], \ldots, [s_n]) = \alpha(s_1, \ldots, s_n)$$

となるものが唯一つ存在する。

すなわち、商写像 q が $\alpha, \bar{\alpha}$ を保つような $\bar{\alpha}$ が唯一つ存在する。

例 2.3.12. $(M_n(\mathbb{R}), \times, E_n)$ はモノイドである。ここに E_n は n 次単位行列である。

n 次正方行列の下に一行と右に一列、0 のみからなる行と列を付け加える写像 $f : M_n(\mathbb{R}) \to M_{n+1}(\mathbb{R})$ は、積に関して半群の準同型であるがモノイドの準同型ではない。単位元が単位元にうつされないからである。

定義 2.3.13. $(S, \circ_S, e_S)$ をモノイドとする。$\mathrm{id}_S : S \to S$ はモノイド準同型となり、**恒等射**と呼ばれる。

$(T, \circ_T, e_T)$ もモノイドとする。モノイド準同型 $f : S \to T$ と $g : T \to S$ であって

$$g \circ f = \mathrm{id}_S, \quad f \circ g = \mathrm{id}_T$$

となるものがあるとき、g を f の、f を g の逆射という。逆射を持つような準同型を可逆射、または同型射、同型写像、または単に同型という。モノイドであることを強調してモノイド同型ともいう。

このような状況のとき、モノイド S と T はモノイドとして同型であるという。

半群の場合の定義 2.2.5 と全く同じであることに注意してほしい。

注意 2.3.14. カテゴリー論（圏論）を学ぶと、逆射の定義を統一することができる。

命題 2.3.15. $f : S \to T$ がモノイド準同型でかつ全単射であるとする。このとき、f の逆写像 g が存在し、$g : T \to S$ もモノイド準同型となり、したがって f の逆射となる。

証明. g が半群準同型であることは命題 2.2.6 から従う。あとは $g(e_T) = e_S$ を言えばよい。f は単射なので、両辺を f で送って一致することを見ればよい。左辺の行先は $f(g(e_T)) = e_T$ (f が g の逆写像であるから)、右辺の行先は $f(e_S) = e_T$ (f が単位元を保つから) なので、一致する。 □

定義 2.3.16. S, S' をモノイドとする。S から S' へのモノイド準同型 (monoid homomorphism) の集合を

$$\mathrm{Hom}_{\mathrm{monoid}}(S, S')$$

で表す。特に、$S = S'$ のとき

$$\mathrm{End}_{\mathrm{monoid}}(S) := \mathrm{Hom}_{\mathrm{monoid}}(S, S)$$

とおいて S のモノイド自己準同型 (monoid endomorphism) の集合という。$(\mathrm{End}_{\mathrm{monoid}}(S), \circ, \mathrm{id}_S)$ はモノイドとなる。

なお、定義 2.2.7 に現れる $(\mathrm{End}_{\mathrm{semigp}}(S), \circ, \mathrm{id}_S)$ や $(\mathrm{End}_{\mathrm{magma}}(S), \circ, \mathrm{id}_S)$ もモノイドである。

2.3.4　部分モノイド

定義 2.3.17. (部分モノイド)　モノイド $(S, \circ, e_S)$ の部分モノイドとは、S の部分集合 T であって、T が $\circ$ について閉じていて、かつ $e_S \in T$ であるものを言う。このとき $(T, \circ, e_S)$ はモノイドとなる。このモノイドを部分モノイドという。

証明. 証明するべきことは $(T, \circ, e_S)$ がモノイドになるということである。半群の場合の命題 2.2.9 により部分半群となる。あと、やるべきことは e_S が半群 $(T, \circ)$ の単位元であること ([G2]) を示すことである。が、これは命題 2.2.9 の証明であらわれた「S で成り立っているんだから、その部分である T でも成り立つ」という理屈により自動的に成り立つ。

ここでも公理 [G2] は自動的に成り立ってしまう。 □

問題 2.14. $(M_n(\mathbb{R}), \times, E_n)$ を正方行列が積についてなすモノイドとする。この部分集合 S として、右端の列と最下段の列が 0 であるようなものを考える。$(S, \times)$ はモノイドであることを示せ。$(S, \times)$ は $(M_n(\mathbb{R}), \times)$ の部分半群であるが、部分モノイドではないことを示せ。

注意 2.3.18. この問題が示唆するところは、マグマや半群の場合（命題 2.2.9）と異なり、「モノイド S の部分集合 T は、$\circ$ で閉じているだけでは部分モノイドにはかならずしもならない」ということである。この問題の例では、T が単位元を持っていて、したがって T 自身がモノイドであるのに、S の部分モノイドではない。この違いは、「モノイドに単位元という演算 (0 項演算) が指定されていること」に起因する。モノイド S の部分集合 T が部分モノイドであるためには、$\circ$ で閉じているのみならず、「S の単位元を含んでいること」が必要となる。言い換えると、「S で単位元をとるという 0 項演算について、T が閉じていること」が必要である。

くどい説明で恐縮だが、一般的な定義「モノイドとは、単位元を持つ半群である」を採用すると、上の例を「部分モノイドではない」と主張できなくて困る。本書のように、単位元をモノイドの構造の一つとみなす方が自然である。

問題 2.15. S を集合、$\alpha : S^n \to S$ を n 項演算とする。$T \subset S$ が演算 α に閉じているとは、

$$\forall t_1, \ldots, t_n \in T \quad \alpha(t_1, \ldots, t_n) \in T$$

が成り立つことである。$n = 0$ の場合を考察することで、部分モノイドの定義に現れた $e_S \in T$ なる条件が、「T が 0 項演算 e に閉じている」と言い換えられることを示せ。

例 2.3.19. 例 2.2.10 で見た半群とその部分半群は、全てモノイドとその部分モノイドとなっている。

2.3.5　商モノイド

モノイド $(S, \circ, e_S)$ の台集合 S に、二項演算 $\circ$ とコンパチブルな同値関係があるとき、商集合は自動的にモノイドとなる。これを商モノイドという。半群の場合の定理 2.2.11 参照。

定理 2.3.20. $(S, \circ, e_S)$ をモノイドとし、$\sim$ を S 上の同値関係とする。商写像

$$q : S \to S/\sim$$

がモノイド準同型となるような二項演算 $\bar{\circ}$ ならびに 0 項演算 $\bar{e_S}$ が $S/\sim$ に定義される必要十分条件は、$\circ$ と $\sim$ がコンパチブルである (系 1.3.23 参照) ことである。

このとき、$\bar{\circ}, \bar{e_S}$ はただ一通りに定まる。$(S/\sim, \bar{\circ}, \bar{e_S})$ を S の $\sim$ による**商モノイド** (quotient monoid) といい、q を商準同型と言う。

証明. 十分性を示す。定理 2.2.11 によれば、q が半群準同型となるような $S/\sim$ の二項演算 $\bar{\circ}$ がただ一つ存在する。あとは、q がモノイド準同型になるような $S/\sim$ の単位元 $\bar{e_S}$ がただ一つ存在することを示せばよい。

q がモノイド準同型であることから、単位元は単位元に移る。よって、$\bar{e_S} = [e_S](= q(e_S))$ となるしかない。これで、唯一性が言える。あとは $(S/\sim, \bar{\circ}, \bar{e_S})$ が [G2] を満たすことを示せばモノイドとなり、q はモノイド準同型となり、証明が終わる。[G2] の確認は、次のとおり：系 1.3.23 を用いて $[g]\bar{\circ}[e_S] = [g \circ e_S] = [g]$, $[e_S]\bar{\circ}[g] = [e_S \circ g] = [g]$.

必要性は定理 2.1.20 から従う。 □

例 2.3.21. 自然数 m に対し、$\mathbb{Z}$ における和は m を法とする合同関係とコンパチブルである (問題 1.23)。従って定理 2.3.20 により

$$q : \mathbb{Z} \to \mathbb{Z}/m, \quad n \mapsto [n]$$

をモノイド準同型とするようなモノイドの構造 $(\mathbb{Z}/m, \bar{+}, [0])$ が商集合に入る。(命題 1.3.29 により、$\mathbb{Z}/m$ を商集合 $\mathbb{Z}/\equiv$ と同一視している。)

平たくいうなら、$\mathbb{Z}/m$ に $[a]\bar{+}[b] := [a+b]$ で和を定義することができ、$[0]$ を単位元とするモノイドとなる。

例 2.3.22. 上で、和を積に変えると、次のようになる。

自然数 m に対し、$\mathbb{Z}$ における積 $\times$ は m を法とする合同関係とコンパチブルである (問題 1.23)。従ってモノイドの準同型定理 2.3.20 により

$$q : \mathbb{Z} \to \mathbb{Z}/m, \quad n \mapsto [n]$$

をモノイド準同型とするようなモノイドの構造 $(\mathbb{Z}/m, \bar{\times}, [1])$ が商集合に入る。

平たくいうなら、$\mathbb{Z}/m$ に $[a]\bar{\times}[b] := [a \times b]$ で積を定義することができ、$[1]$ を単位元とするモノイドとなる。

注意 2.3.23. 代数構造一般について、次が言える：「指定された演算のすべてが、同値関係とコンパチブルである」ならば、商集合におなじ代数構造が入る。(より詳しく言えば、商写像が準同型となるような構造が入る。そして、そのような構造があることと、コンパチビリティは同値である。)

しかるにモノイドの場合、準同型定理において「単位元と $\sim$ のコンパチビリティ」が現れていない。0 項演算とのコンパチビリティはどうなったのか。というと、0 項演算の特殊事情「0 項演算と同値関係は、常にコンパチブルである」が成立するので、この条件を加えても加えなくてもおなじ定義になる。

問題 2.16. 0 項演算と同値関係は、常にコンパチブルであることを示せ。

2.3.6　モノイドの準同型定理

定理 2.3.24. $(X, \circ_X, e_X)$ をモノイドとし、$\sim$ を X 上の $\circ_X$ とコンパチブルな同値関係とする。$(X/\sim, \bar{\circ}, \bar{e_X})$ で商モノイドを表す。$q : X \to X/\sim$ を商準同型とし、任意のモノイド $(Y, \circ_Y, e_Y)$ と任意のモノイド準同型 $f : X \to Y$ を考える。

$\sim$ が f とコンパチブルである、すなわち任意の $x, x' \in X$ に対し

$$x \sim x' \Rightarrow f(x) = f(x')$$

となるならば、定理 1.3.20 により写像 $\bar{f} : X/\sim \to Y$ であって、

$$f = \bar{f} \circ q$$

なる性質をもつものがただ一つ存在するが、$\bar{f}$ はモノイド準同型である。

この状況を、モノイド準同型 f は同値関係 $\sim$ とコンパチブルであるといい、また $\bar{f}$ が well-defined であるという。

証明. 定理 2.2.12 と比べることにより、必要性はあきらか。十分性は、「半群準同型 $\bar{f}$ がモノイド準同型であること」を示せばよいが、

$$\bar{f}([e_X]) = f(e_X) = e_Y$$

より従う。最初の等号で $f = \bar{f} \circ q$ を用い、次の等号で f が単位元を保つことを用いた。 □

定理 2.3.25. (モノイドの準同型定理)

$(X, \circ_X, e_X)$、$(Y, \circ_Y, e_Y)$ をモノイドとし、$f : X \to Y$ なるモノイド準同型が与えられたとする。$f(X) \subset Y$ で f による X の像を表す。このとき、

1. $f(X)$ は Y の部分モノイドである。
2. $\sim_f$ は $\circ$ とコンパチブルな同値関係である。したがって、$X/\sim_f$ は商モノイドとなる。
3. f が
$$X \xrightarrow{q} X/\sim_f \xrightarrow{\bar{f}} Y$$
なる合成となるような $\bar{f}$、すなわち
$$f = \bar{f} \circ q$$
なる $\bar{f}$ がただ一つ存在するが、これはモノイド準同型となる。そして、その終集合を $f(X)$ に制限して得られる
$$\bar{f} : X/\sim_f \to f(X)$$
はモノイド同型となる。

（つまり、定理 2.2.13 は「半群」を「モノイド」に変えてもそのまま成り立つ。）

証明. 定理 2.2.13 に加えて何を余計に示さないとならないかのみ述べる。

1. 部分半群であることは示されている。部分モノイドであること、すなわち $e_Y \in f(X)$ を示さないとならない。が、$f(e_X) = e_Y$ より従う。

2. 商モノイドとなることは定理 2.3.20 で示されている。

3. $\bar{f}$ が半群準同型であることは示されている。あとはモノイド準同型であることを示さなくてはならない。が、$\bar{f}([e_X]) = e_Y$ より従う。

□

2.3.7 0 を含む自然数と指数法則

半群においては、$n \in \mathbb{N}$ に対して

$$g^n := g \circ g \circ g \circ \cdots \circ g \quad (n \text{ 個})$$

が定義された。これを $n = 0$ のときに拡張するにはどうするのが妥当か。$(\mathbb{N}, +)$ は半群であり、モノイドではなかった。0 も付け加えると $(\mathbb{N} \cup \{0\}, +, 0)$ はモノイドとなる。そこで、$(S, \circ, e_S)$ をモノイドとするとき、

$$(\mathbb{N} \cup \{0\}, +, 0) \to (S, \circ, e_S), \quad n \mapsto g^n$$

がモノイドの準同型となるように g^0 を定義することが、系 2.2.15 との対応からすると妥当に思える。すると単位元は単位元に行かなくてはならない ([HC]) から、

$$g^0 = e_S$$

と定義することになる。

定理 2.3.26. (指数法則)
$(S, \circ, e_S)$ をモノイドとし、$g \in S$ を一つの元とする。0 以上の整数 n, m に対し次が成立する。

$$(g^n) \circ (g^m) = g^{n+m}.$$

但し、$g^0 = e_S$ と定義する。

問題 2.17. 定理 2.2.14 を使って、上の定理を証明せよ。

系 2.3.27. $(S, \circ, e_S)$ をモノイドとし、$g \in S$ を一つの元とする。このとき、

$$f : (\mathbb{N} \cup \{0\}, +, 0) \to (S, \circ, e_S)$$

なるモノイド準同型であって、$1_{\mathbb{N}\cup\{0\}} \mapsto g$ となるものが唯一つ存在する。

証明. 存在したとすると、モノイド準同型は半群準同型でもあるので、f は半群準同型。$(\mathbb{N}, +) \subset (\mathbb{N} \cup \{0\}, +)$ は部分半群である。よって、$f|_{\mathbb{N}}$ (f を $\mathbb{N}$ に制限したもの) は $(\mathbb{N}, +) \to (S, \circ)$ なる半群の準同型である。$n > 0$ に対しては系 2.2.15 により

$$f(n) = g^n$$

となる。また、モノイド準同型であるということから単位元 0 は単位元 e_S に移される、すなわち $f(0) = g^0 = e_S$。これで一意性が言えた。

これがモノイド準同型になるということが、上の指数法則 2.3.26 の主張するところである。 □

2.4　群

2.4.1　逆元と群

定義 2.4.1. $(S,\circ)$ を単位元 e_S を持つマグマとする。（単位元はあれば一つであること、すなわち問題 2.12 に注意。）$g\in S$ の（e に関する）**左逆元** a とは、

$$a\circ g=e_S$$

を満たす $a\in S$ のことをいう。$g\in S$ の**右逆元** b とは、

$$g\circ b=e_S$$

を満たす $b\in S$ のことをいう。g の左逆元であって、かつ右逆元であるような元を g の**逆元** という。すなわち、

$$a\circ g=e_S, g\circ a=e_S$$

となるような a のことである。逆元を持つ元を**可逆元** という。

命題 2.4.2. $(S,\circ,e_S)$ をモノイドとする。g に左逆元 a と右逆元 b が存在するならば、それらは一致する。特に、g の逆元は存在すれば唯一つ。これを g^{-1} で表す。

証明.

$$a=a\circ e_S=a\circ(g\circ b)=(a\circ g)\circ b=e_S\circ b=b.$$

よって左逆元と右逆元は、両方存在すれば一致する。

特に、逆元が二つあったとしよう。それらを a,b とすれば、a は左逆元でもあるし、b は右逆元でもあるから、上の事実より一致せざるを得ない。 □

モノイドの代わりに、条件を弱めて「単位元をもつマグマ」に対しても、逆元が存在すれば唯一つであることが証明できるか？実は、反例がたくさんあり、当然証明はできない。例えば $(\mathbb{R},*)$ を

$$x*y=x+y+x^2y^2$$

で定義するとこれはマグマであり、0 が単位元となっている。

$$x*y=0$$

を二次方程式の解の公式を用いて解くと、逆元が二つ存在することがあることがわかる。

2.4.2　群の定義

ようやく群の定義を述べる段になった。「群とは、モノイドであって、全ての元に逆元が存在するものを言う」というのが通常の定義である。本書では、（同値な定義だが）次のように「どの演算が群という代数構造に指定されているか」を明示する。

定義 2.4.3.（**群**、group）
群 G とは、材料として

GA 集合 G_0(台集合などと呼ばれる)

GB G_0 上の二項演算 $\circ$(積、合成などと呼ばれる)

GC $e \in G_0$(単位元と呼ばれる)

GD G_0 上の単項演算 $g \to g^{-1}$(逆元を取る演算と呼ばれる)

が与えられて、次の三つの性質 (群の公理と呼ばれる) を満たすもの。

G1 (結合法則, associative law)

$$g_1, g_2, g_3 \in G_0 \Rightarrow (g_1 \circ g_2) \circ g_3 = g_1 \circ (g_2 \circ g_3)$$

G2 (単位元の法則, unit law)

$$g \in G_0 \Rightarrow g \circ e = g, e \circ g = g$$

G3 (逆元の法則, inverse law)

$$g \circ g^{-1} = e \text{ かつ } g^{-1} \circ g = e$$

群 $G = (G_0, \circ, e, ()^{-1})$ と表す。台集合 G_0 を、しばしば G であらわす。

注意 2.4.4. $(G_0, \circ)$ を半群とする。もし、これに単位元があったらそれは唯一つであるのだから、単位元を敢えて指定せずに「$(G_0, \circ)$ はモノイドである」という言い方をした。これは「半群であって単位元がある」ということを指している。さらに、$(G_0, \circ)$ をモノイドとするとき、「G_0 の全ての元に逆元がある」ということがわかれば、逆元は存在すれば唯一つに決まる (命題 2.4.2) のであるから、$G_0 \to G_0, \quad g \mapsto g^{-1}$ なる単項演算は決まる。なので、群 G は、$(G_0, \circ)$ だけ与えれば復元できる。そのため、「群 $(G_0, \circ)$」と表すことが多い。

同じ理由で、多くの教科書では「半群であって、単位元をもち、全ての元が逆元を持つものを群という」という定義を採用している。しかし、本書の定義の方が現代的である。本書の内容だけではうまく説明できないが、「カテゴリーにおける群対象」という概念があり、上記の意味での群は「集合のカテゴリーにおける群対象」と一致する。群対象を定義する際には、例えば「逆元が存在する」という公理ではなく、「逆元をとる演算がそのカテゴリーの射として与えられている」という公理をおく。このやり方の方が広く使える。

問題 2.18. 例 2.3.4 に挙げられたモノイドが、群であるかどうか調べよ。

注意 2.4.5. 数の概念が歴史的に発展してきた様子は、半群→モノイド→群という概念の進化に奇妙に対応している。

自然数 $(\mathbb{N}, +)$ は半群であるがモノイドではない。単位元が存在しないからである。そこで、0 という概念を発明（発見？）して $(\mathbb{N} \cup \{0\}, +, 0)$ とすると、これはモノイドとなる。

しかし、これは群にはならない。和に関する逆元、すなわち x に対する $-x$ が存在しないからである。そこで、負の数を発明（発見？）して $(\mathbb{Z}, +, 0)$ とすると、これは群になった。

一方、$(\mathbb{N}, \times, 1)$ はモノイドである。が、群ではない。積に関する逆元、すなわち $n \in \mathbb{N}$ に対する n^{-1} がないからである。そこで、n^{-1} を考える必要が出てくる。積について閉じているためには、$n^{-1} \times m$ も必要となる。これらを合わせて正の有理数 $\mathbb{Q}_{>0}$ を考えると、$(\mathbb{Q}_{>0}, \times, 1)$ は群となる。

定義 2.4.6. 群 $(G, \circ)$ が**可換群** (commutative group) であるとは、[G1]-[G3] のほかにさらに

G4 （可換則, commutativity law）

$$\forall g_1, g_2 \in G \quad g_1 \circ g_2 = g_2 \circ g_1$$

が成立すること。

可換群のことをアーベル群 (abelian group) ともいう。これは、群論の創始者の一人である Abel にちなんだ命名である。

注意 2.4.7. アーベル群に関しては、二項演算を $+$ で書くことも多い。はなはだご都合主義ではあるが、二項演算を $+$ で記述したアーベル群のことを**加法群** (additive group) とよぶ。加法群においては、単位元を 0 であらわしてゼロ元と呼ぶ。g の逆元を $-g$ であらわす。

例 2.4.8. 例 2.3.21 に見たモノイド

$$(\mathbb{Z}/m, \bar{+}, [0])$$

は群である。全ての元が可逆であることさえ言えばよいのであるが、

$$[a]\bar{+}[-a] = [a + (-a)] = [0], \quad [-a]\bar{+}[a] = [(-a) + a] = [0]$$

であるから $[a]$ の逆元として $[-a]$ が取れる。

$\mathbb{Z}/m$ においては、$\bar{+}$ は単に $+$ で表され、またしばしば $[a]$ を単に a と書いてしまったりする。例えば、「$\mathbb{Z}/5$ においては $1 + 4 = 0$」などと書く。本来なら「$[1]\bar{+}[4] = [0]$」と書くべきところではある。

問題 2.19.

1. $(G, \circ)$ をモノイドとする。$g, h \in G$ がどちらも可逆のとき、$g \circ h$ も可逆であり、

$$(g \circ h)^{-1} = h^{-1} \circ g^{-1}$$

であることを示せ。

2. $(G, \circ)$ をモノイドとする。$g \in G$ が可逆であるとき、g^{-1} も可逆であり、その逆元 $(g^{-1})^{-1}$ は g となることを示せ。

上の問題 2.19 から、次のことがわかる。

命題 2.4.9. $(G, \circ, e)$ をモノイドとする。G の可逆元の全体を H とすると、$(H, \circ, e)$ は群となる。この群を、モノイド G の**可逆元のなす群**といい、しばしば $G^\times$ であらわす。

証明.

H が部分モノイドであること：

問題 2.19 の 1 によれば、$g, h \in H$ ならば $g \circ h \in H$ である。また、e の逆元は e 自身であるから $e \in H$。定義 2.3.17 により、H は G の部分モノイドとなる。

H が群であること：

H の元はモノイド G の可逆元であるが、実はモノイド H の可逆元でもあることが、次のようにわかる。$h \in H$ ならば h^{-1} は可逆 (問題 2.19 の 2) であるから H の定義により $h^{-1} \in H$ となる。すなわち $h \in H$ の逆元が H の中にあるので、$(H, \circ, e)$ は群となる。

□

例 2.4.10. 実 n 次正方行列の集合 $M_n(\mathbb{R})$ は、積についてモノイドになっている。これに対して命題 2.4.9 を使うと、「可逆な n 次正方行列全体は積について群をなす」ことがわかる。この群を $GL_n(\mathbb{R})$ であらわし、n 次**実行列群**または n 次**実一般線形群** (real general linear group) とよぶ。

$(M_n(\mathbb{R}), \times)$ を行列が積に関してなすモノイドとすれば、

$$GL_n(\mathbb{R}) := M_n(\mathbb{R})^\times$$

である。

注意 2.4.11. 上のことは、一般には体 K を成分とする行列について言えることである。例えば、成分が全て有理数であるような可逆な n 次正方行列の全体は積について $GL_n(\mathbb{Q})$ と表される群をなす。

注意 2.4.12. 可逆な行列は、正則行列とも呼ばれる。

例 2.4.13. X を集合とし、$\mathrm{Map}(X, X)$ を X から X への写像の全体とすると、$(\mathrm{Map}(X, X), \circ, \mathrm{id}_X)$ はモノイドである (例 2.3.4 参照)。これに対して上の命題 2.4.9 を使うと、$\mathrm{Map}(X, X)^\times$、すなわち X から X への可逆な写像全体 (全単射全体といっても同じ) は合成について群をなすことがわかる。この群を X **上の対称群**といい、S_X であらわす。特に、$X = \{1, 2, \ldots, n\}$ のとき、この群を n **次対称群**といい S_n であらわす。

例 2.4.14. $(\mathbb{Z}/m, \bar{\times}, [1])$ はモノイドであるので、命題 2.4.9 よりその可逆元の全体 $((\mathbb{Z}/m)^\times, \bar{\times}, [1])$ は群である。

例 2.4.15.

1. $(\mathbb{Z}, \times, 1)$ の可逆元がなす群 $\mathbb{Z}^\times$ は $\{1, -1\}$ なる二元が積についてなす群である。実際、$\mathbb{Z}$ における積に関する可逆元 x とは、

   $$ax = xa = 1$$

   となる $a \in \mathbb{Z}$ が存在するような $x \in \mathbb{Z}$ である。これは ± 1 に他ならない。

2. $(\mathbb{Q}, \times, 1)$ の可逆元がなす群 $\mathbb{Q}^\times$ は

   $$\mathbb{Q}^\times = \{x \in \mathbb{Q} | x \neq 0\}$$

   である。0 以外の有理数はみな積の逆元を持つからである。

   同様に、$\mathbb{R}^\times$, $\mathbb{C}^\times$ もそれぞれ $\mathbb{R}$、$\mathbb{C}$ から 0 を除いたものとなる。

命題 2.4.9 は自明に近いものであるが、それに続く例を見ると、行列群や対称群といった「全く違う性格の群」の構成に、共通に使えることがわかる。それぞれについて、群であることを確かめる必要がなくなる。モノイドや群という「抽象化」が有効な、一つの例である。

問題 2.20.

1. モノイド $(G, \circ)$ と $g, h \in G$ であって、$g \circ h$ は可逆であるが、g も h も可逆でない例を示せ。
2. A, B を n 次実正方行列とする。AB が正則行列であれば、A も B も正則行列であることを示せ。

モノイドにおいては、可逆元は移項できる。

命題 2.4.16. $(G, \circ, e)$ をモノイドとする。$a \in G$ が可逆元であるとき、方程式

$$a \circ x = b$$

の解は唯一つ存在し

$$x = a^{-1} \circ b$$

である。言い換えれば

$$a \circ x = b \Leftrightarrow x = a^{-1} \circ b.$$

証明. 等式 $a \circ x = b$ の両辺に左から a^{-1} をほどこすと

$$a^{-1} \circ (a \circ x) = a^{-1} \circ b$$

ここで左辺は

$$a^{-1} \circ (a \circ x) = (a^{-1} \circ a) \circ x = e \circ x = x$$

だから $x = a^{-1} \circ b$ が従う。
逆に $x = a^{-1} \circ b$ に左から a をほどこすと $a \circ x = b$ が言える。 □

このように、中学校のころから慣れ親しんだ「移項」という概念は、じつはモノイド一般についての概念である。

2.4.3　群準同型

群から群への群準同型とは、台集合間の写像であって、与えられた 3 種の演算 [GB][GC][GD] を保つものである。

定義 2.4.17. $(S, \circ_S, e_S, ()^{-1})$, $(T, \circ_T, e_T, ()^{-1})$ を群とする。S から T への**群準同型**とは、$f : S \to T$ なる写像であって

HB $\forall s, s' \in S, \quad f(s \circ_S s') = f(s) \circ_T f(s')$

HC $f(e_S) = e_T$

HD $\forall s \in S, \quad f(s^{-1}) = f(s)^{-1}$

の三つをみたすもの。

例 2.4.18. 先に見た例 2.3.6 における

$$\exp : (\mathbb{R}, +, 0) \to (\mathbb{R}^\times, \times, 1)$$

は群準同型である。モノイド準同型であることは先にみた。逆元を逆元に移すことは

$$\exp(-a) = \exp(a)^{-1}$$

より従う。

命題 2.4.19. $(S, \circ_S, e_S)$ と $(T, \circ_T, e_T)$ が群であるとする。このとき、それらをマグマと見てのマグマ準同型 $f : S \to T$ は群準同型である。

言い換えるならば、[HB] だけを確かめれば群準同型であるといえる。

証明. マグマ準同型であるのだから [HB] は言えている。[HC] を言う。

$$f(e_S) = f(e_S \circ_S e_S) = f(e_S) \circ_T f(e_S)$$

である。ここで、T は群であるのだから $f(e_S)^{-1}$ がある。これを上の等式の両辺の右から掛けると

$$f(e_S) \circ_T (f(e_S)^{-1}) = (f(e_S) \circ_T f(e_S)) \circ_T (f(e_S)^{-1})$$

左辺は逆元の定義より e_T。右辺は結合律を使って計算すると

$$f(e_S) \circ_T (f(e_S) \circ_T (f(e_S)^{-1})) = f(e_S) \circ_T e_T = f(e_S)。$$

よって [HC] が言えた。

[HD] を言う。

$$f(e_S) = f(s \circ_S s^{-1}) = f(s^{-1} \circ_S s)$$

である。左辺に [HC] を用い、中辺と右辺に [HB] を用いれば

$$e_T = f(s) \circ_T f(s^{-1}) = f(s^{-1}) \circ_T f(s)$$

となるが、これは逆元の定義 2.4.1 より $f(s^{-1})$ が $f(s)$ の逆元であることを示している。すなわち

$$f(s^{-1}) = f(s)^{-1}.$$

□

命題 2.4.20. $(S, \circ_S)$, $(T, \circ_T)$ をモノイドとし、$f : S \to T$ をモノイド準同型とする。すると $s \in S^\times$ のとき $f(s)$ は T で可逆で $f(s)^{-1} = f(s^{-1})$ が成立する。

従って f は $S^\times$ の元を $T^\times$ の元に移し、$f : S^\times \to T^\times$ なる群準同型を引き起こす。

証明. $s \in S^\times$ とする。

$$e_T = f(e_S) = f(s \circ_S s^{-1}) = f(s^{-1} \circ_S s)$$

であるが、[HB] を使うと

$$e_T = f(s) \circ_T f(s^{-1}) = f(s^{-1}) \circ_T f(s)$$

であるから $f(s^{-1})$ は $f(s)$ の逆元である。言い換えると

$$f(s)^{-1} = f(s^{-1}).$$

特に $f(s)$ は T の中で可逆となり、$f(s) \in T^\times$。

すると f の制限は群から群への写像 $f : S^\times \to T^\times$ なる写像を与えるが、これは [HB] を満たすので命題 2.4.19 より群準同型となる。 □

定義 2.4.21. $(S, \circ_S, e_S, ()^{-1}))$ が群であるとき、恒等写像 id_S は群準同型である。S の**恒等射**という。

$(T, \circ_T, e_T, ()^{-1}))$ も群とする。群準同型 $f : S \to T$ と $g : T \to S$ であって

$$g \circ f = \mathrm{id}_S, \quad f \circ g = \mathrm{id}_T$$

となるものがあるとき、g を f の、f を g の**逆射** (inverse homomorphism) という。逆射を持つような準同型を**可逆射**、または**同型射**、**同型写像**、または単に**同型**という。群であることを強調して**群同型** ともいう。

群 $(S, \circ_S, e_S, ()^{-1})$ と $(T, \circ_T, e_T, ()^{-1})$ の間に同型写像があるとき、これらの群は**同型**であるという。

命題 2.4.22. $(S, \circ_S, e_S)$ から $(T, \circ_T, e_T)$ への群準同型写像 f が全単射ならば群同型である。

証明. 群準同型とは群の間のマグマ準同型のことである (命題 2.4.19)。ゆえに命題 2.1.13 から直ちに従う。 □

2.4.4　部分群

定義 2.4.23. (部分群)

群 $(S, \circ, e_S)$ の部分群とは、S の部分集合 T であって、T が 3 種の演算 $\circ$, e, $()^{-1}$ に閉じているものをいう。平たく言えば、

S1 $\forall t, t' \in T$ に対して $t \circ t' \in T$、

S2 $e \in T$,

S3 $\forall t \in T$ に対して $t^{-1} \in T$

であるものを言う。このとき $(T, \circ, e_S, ()^{-1})$ は群となる。このような群を部分群という。このとき、埋め込み写像 $\iota : T \to S, \quad t \mapsto t$ は群準同型となる。T が S の部分群であることを、まぎらわしい表記ではあるが $T < S$ とあらわす。

証明. $(T, \circ, e_S)$ は定義 2.4.23 によりモノイドであるから、群になることを示すには逆元が存在することを示せばよい。$t \in T$ に対し $t^{-1} \in T$ は仮定されているのだから、あとはこれが逆元になること [G3] を示せばよい。しかしまたもや（定義 2.4.23 の下の証明と同じように)、「S で成り立っているんだから、その部分である T でも成り立つ」という理屈により自動的に成り立つ。ここでも公理 [G3] は自動的に成り立ってしまう。

ι が群準同型であることは容易に確かめられる。 □

2.4.5 商群

群の台集合に、二項演算とコンパチブルな同値関係があるとき、商集合は自動的に群となる。これを商群という。モノイドの場合の定理 2.3.20 参照。

定理 2.4.24. $(S, \circ, e_S)$ を群とし、$\sim$ を S 上の同値関係とする。商写像

$$q : S \to S/\sim$$

が群準同型となるような二項演算 $\bar{\circ}$ と 0 項演算 $\bar{e_S}$ と単項演算 $()^{-1}$ が $S/\sim$ に定義される必要十分条件は、$\circ$ と $\sim$ がコンパチブルである (系 1.3.23 参照) ことである。

このとき、$\bar{\circ}$ はただ一通りに定まる。$(S/\sim, \bar{\circ}, \bar{e_S})$ を S の $\sim$ による商群といい、q を商準同型と言う。

証明. 群準同型であればモノイド準同型である。よって、定理 2.3.20 の必要性の部分により、必要性はわかる。十分性について示す。$\sim$ と $\circ$ がコンパチブルであれば、同じ定理の十分性の部分により $q : S \to S/\sim$ をモノイド準同型とするモノイド構造 $(S/\sim, \bar{\circ}, [e_s])$ がただ一つ存在する。ここで、q はモノイド準同型であるから命題 2.4.20 により可逆元を可逆元に移す。よって、q の像の元は $S/\sim$ の可逆元となる。ここで、S の元は全て可逆で q は全射だから $S/\sim$ の元も全て可逆となり、$S/\sim$ は群である。q は群の間のマグマ準同型だから命題 2.4.19 により群準同型となる。 □

2.4.6 普遍代数

この手の定理 2.4.24, 2.3.20, 2.2.11, 2.1.20 は、実は統一的に証明できる。

「代数構造の与えられた集合」という言葉で、次のような材料と公理の組を考える。まず材料は $(S, \alpha_{1,S}, \ldots, \alpha_{m,S})$ である。ここに S は集合、$\alpha_{i,S}$ は演算（何項演算でも良い、n_i 項演算であるとしよう）である。

例えば、群 $(S, \circ, e_S, ()^{-1})$ では、α_1 が二項演算、α_2 が 0 項演算、α_3 が単項演算である。

次に、公理を考える。公理は、「全ての $s_1, s_2, \ldots, s_l \in S$ に対し、これらから指定された演算をある特定の順番で繰り返して得られる元と、別の順番で繰り返して得られる元が、常に等しい」という形のものが、いくつか与えられているとする。

注意 2.4.25. この本では、このような公理のことを「無条件等号型の公理」と呼ぶことにする。（標準的用語が無いようである。）普遍代数の分野ではこのような公理で定義された代数系を「equational class」(等式クラス) と呼ぶ。([4, p.75, Definition 11.7].)

例えば、マグマ $(S, \circ)$ が与えられたとき、

$$\forall a, b, c \in S \quad (a \circ b) \circ c = a \circ (b \circ c)$$

は、無条件等号型の公理の例である。群の公理に現れる G1, G2, G3 や可換性 G4 もそのような公理の例となっている。

無条件等号型でない公理の例としては、ちょっと先走っていて申し訳ないが、体の公理にあらわれる

$$s \neq 0 \Rightarrow s^{-1} \in S$$

があげられる。

定義 2.4.26. 代数構造とは、$n_1, n_2, \ldots, n_m$ なる 0 以上の自然数をきめ、それを項数にもつ演算たちと、それらが満たすべき公理を決めたもの。

無条件等号型の代数構造とは、それらの公理が無条件等号型であること。

その代数構造を持つ集合 S とは、$(S, \alpha_1, \ldots, \alpha_m)$ なる組であって、各 α_i は n_i 項演算で、与えられた公理を満たすもの。

例えば、群構造と呼ばれる代数構造は、$\circ$, e, $()^{-1}$ なる 2 項、0 項、単項演算と、それらに関して（無条件等号型の）公理 G1, G2, G3 を与えたものである。

群構造を持つ集合とは、$(S, \circ_S, e_S, ()^{-1})$ の組であって、G1, G2, G3 を満たすものである。すなわち、群である。

定義 2.4.27. $\mathcal{C}$ を代数構造とし、S, T をその代数構造を持つ集合とする。S から T への $\mathcal{C}$ 準同型とは、$f : S \to T$ なる写像であって、指定された全ての演算を保つ（定義 2.3.7 参照）もの。すなわち、

$$\begin{array}{ccc} S^{n_i} & \xrightarrow{f^{n_i}} & T^{n_i} \\ \downarrow \alpha_{i,S} & & \downarrow \alpha_{i,T} \\ S & \xrightarrow{f} & T \end{array}$$

が全ての $i = 1, 2, \ldots, m$ に対して可換なもの。

この定義と命題 2.3.9 より次を得る。

系 2.4.28. $\mathcal{C}$ 準同型二つの合成は、$\mathcal{C}$ 準同型である。

定理 2.4.29. $\mathcal{C}$ を無条件等号型の代数構造とし、S をその構造を与えられた集合とする。$T \subset S$ が、与えられた演算 $\alpha_1, \ldots, \alpha_m$ について閉じているならば、T はこれらの演算によって $\mathcal{C}$ 構造を持つ。S を T の部分 $\mathcal{C}$ 構造という。

証明. 無条件等号型の公理は、演算に閉じていさえすれば部分集合についても成り立つから。 □

定理 2.4.30. $\mathcal{C}$ を代数構造とし、S をその構造を与えられた集合とする。S 上の同値関係 $\sim$ が、与えられた演算 $\alpha_{1,S}, \ldots, \alpha_{m,S}$ 全てとコンパチブルならば、$S/\sim$ には演算 $\bar{\alpha}_1, \ldots, \bar{\alpha}_m$ であって $q : S \to S/\sim$ がこれらの演算を保つものが唯一つ定義される。

$\mathcal{C}$ が無条件等号型ならば、$S/\sim$ はこれらの演算によって $\mathcal{C}$ 構造を持ち、q は $\mathcal{C}$ 準同型となる。このとき $S/\sim$ を S の商 $\mathcal{C}$ 構造という。

証明. 演算 $\bar{\alpha}_i$ の存在は定理 2.3.11 からしたがう。唯一性もそこからしたがう。q が演算を保つこともそこからしたがう。

あとは $\mathcal{C}$ が無条件等号型であるとき、$S/\sim$ がその構造を持つことさえ言えれば、q が準同型であることは定義からしたがう。

$S/\sim$ と $\bar{\alpha}_i$ が公理を満たすことを言えば良いのであるが、これは q の全射性と、公理が無条件等号型であることからしたがう。

具体例でみよう。公理 G3 を確かめてみる。q が全射であることから、$S/\sim$ の任意の元は $[a]$ とあらわされる。わかりやすく（？）するために、$\circ$ を $\alpha(-,-)$ で、e を $\beta()$ で、$()^{-1}$ を $\gamma(-)$ で表してみよう。q が、これらの演算とその$^-$を保つことはもう示したのである。それは

$$q(\alpha(a,b)) = \bar{\alpha}(q(a), q(b)),\ q(\beta()) = \bar{\beta}(),\ q(\gamma(a)) = \bar{\gamma}(q(a))$$

と表せる。われわれの任務は、G3 が $S/\sim$ で成立すること、すなわち

$$\bar{\alpha}(x, \bar{\gamma}(x)) = \bar{\alpha}(\bar{\gamma}(x), x) = \bar{\beta}()$$

が成立することを示すことである。ここで、q の全射性により $x = q(a)$ となるような $a \in S$ が存在するのだから、このような x について上の等式を示せばよい。

しかるに、S においては G3 が成り立つのであるから

$$\alpha(a, \gamma(a)) = \alpha(\gamma(a), a) = \beta().$$

全てに $q()$ を施すと

$$q(\alpha(a, \gamma(a))) = q(\alpha(\gamma(a), a)) = q(\beta())$$

だが、q が演算たちを保つことから、「$q \circ$ 演算 $= \overline{\text{演算}} \circ q$」である。すなわち

$$q(\alpha(a, \gamma(a))) = \bar{\alpha}(q(a), q(\gamma(a))) = \bar{\alpha}(q(a), \bar{\gamma}(q(a)))$$

であるから、ほかの項も計算すれば

$$\bar{\alpha}(q(a), \bar{\gamma}(q(a))) = \bar{\alpha}(\bar{\gamma}(q(a)), q(a)) = \bar{\beta}()$$

である。これが示したい、$S/\sim$ における G3 であった。 □

このように、代数構造一般を扱う数学の分野を普遍代数 (universal algebra) という。

2.4.7 群の準同型定理：準備段階

いままで集合・マグマ・半群・モノイドの準同型定理を述べてきた。群についても次のように同じ形の定理が成立する。しかし、後述するように、群については「正規部分群」による定式化が通常行われており、そちらを「群の準同型定理」と呼ぶのが普通である (定理 2.4.76, 定理 2.4.77, 定理 2.4.78 参照)。そのため、この節では「準備段階」という言葉を付加した。

定理 2.4.31. $(X, \circ_X, e_X)$ を群とし、$\sim$ を X 上の $\circ_X$ とコンパチブルな同値関係とする。$(X/\sim, \bar{\circ}, e_{\overline{X}})$ で商群を表す。$q : X \to X/\sim$ を商準同型とし、任意の群 $(Y, \circ_Y, e_Y)$ と任意の群準同型 $f : X \to Y$ を考える。

f と $\sim$ がコンパチブル、すなわち任意の $x, x' \in X$ に対し

$$x \sim_X x' \Rightarrow f(x) = f(x')$$

であれば定理 1.3.20 により $\bar{f} : X/\sim_X \to Y$ であって、

$$f = \bar{f} \circ q$$

なる性質をもつものが唯一つ存在するが、これは群準同型である。

この状況を、群準同型 f は同値関係 $\sim_X$ にコンパチブルであるといい、また $\bar{f}$ が well-defined であるという。

証明. 定理 2.3.24 と比べると、「モノイド準同型 $\bar{f}$ が群準同型であること」を示せばよいが、命題 2.4.19 より明らか。 □

注意 2.4.32. この定理も、普遍代数 (§2.4.6) の枠組みで一般的に述べられる。

$\mathcal{C}$ を代数構造とし、S,T をその構造の与えられた集合とする。$f : S \to T$ を $\mathcal{C}$ 準同型とし、$\sim$ を S 上の同値関係で与えられた全ての演算とコンパチブルなものとする。

このとき、$\bar{f} : S/\sim \to T$ なる写像で $f = \bar{f} \circ q$ なるものが唯一つ存在するが、これは全ての演算 $\bar{\alpha}_{i,S}$, $\alpha_{i,T}$ を保つ $(i = 1, \ldots, m)$。実際、

$$\begin{aligned}&\bar{f}(\bar{\alpha}_{i,S}(q(s_1), \ldots, q(s_{n_i}))) = \bar{f}(q(\alpha_{i,S}(s_1, \ldots, s_{n_i}) = f(\alpha_{i,S}(s_1, \ldots, s_{n_i}))\\ &= \alpha_{i,T}(f(s_1), \ldots, f(s_{n_i})) = \alpha_{i,T}(\bar{f}(q(s_1)), \ldots, \bar{f}(q(s_{n_i})))\end{aligned}$$

である。

特に、$\mathcal{C}$ が無条件等号型の代数構造であれば、$S/\sim$ は定理 2.4.30 により $\mathcal{C}$ の構造をもち、$\bar{f}$ は $\mathcal{C}$ 準同型となる。

定理 2.4.33. (群の準同型定理:準備段階)

$(X, \circ_X, e_X)$、$(Y, \circ_Y, e_Y)$ を群とし、$f : X \to Y$ なる群準同型が与えられたとする。$f(X) \subset Y$ で f による X の像を表す。このとき、

1. $f(X)$ は Y の部分群である。
2. $\sim_f$ は $\circ$ とコンパチブルな同値関係である。したがって、$X/\sim_f$ は商群となる。
3. f が
$$X \overset{q}{\to} X/\sim_f \overset{\bar{f}}{\to} Y$$
なる合成となるような $\bar{f}$、すなわち
$$f = \bar{f} \circ q$$
なる $\bar{f}$ がただ一つ存在するが、これは群準同型である。そして、その終集合を $f(X)$ に制限して得られる
$$\bar{f} : X/\sim_f \to f(X)$$
は群同型となる。

つまり、定理 2.3.25 は群に対してもそのまま成り立つ。

証明. 定理 2.3.25 に加えて何を余計に示さないとならないかのみ簡単に述べる。

1. 部分モノイドであることは示されている。部分群であることを示すのに、$f(X)$ が逆元をとることに閉じていることを言えばよい。これは、$f(x)^{-1} = f(x^{-1})$ より直ちに従う。
2. 余計に示さないとならないことは存在しない。
3. 命題 2.4.19 により、余計に示さないとならないことは存在しない。

□

注意 2.4.34. これらの準同型定理 2.4.33, 2.3.25, 2.2.13, 2.1.23 も、実は普遍代数の言葉で統一的に述べられる。

$\mathcal{C}$ を無条件等号型の代数構造とし、S,T をその構造の与えられた集合、$f : S \to T$ を準同型とする。このとき、$f(S)$ は T の部分 $\mathcal{C}$ 構造となり、$\sim_f$ は $\mathcal{C}$ により指定された S の全ての演算とコンパチブルな二項関係で、従って商 $\mathcal{C}$ 構造 $S/\sim$ を定める。ここで、集合の準同型定理 1.3.33 により与えられる写像

$$\bar{f} : S/\sim \to f(S)$$

は、$\mathcal{C}$ 構造の同型である。

証明. $f(S)$ が T の指定された演算について閉じていることは、f がその演算を保つことから従う。これと定理 2.4.29 から、$f(S)$ は T の部分 $\mathcal{C}$ 構造を持つ。

同値関係 $\sim_f$ が指定された演算とコンパチブルであることも、その演算を f が保つことから従う。これと定理 2.4.30 から、$S/\sim$ は S の商 $\mathcal{C}$ 構造である。

$\bar{f}$ は全単射であるが、注 2.4.32 によりこれは $\mathcal{C}$ 準同型である。

$\mathcal{C}$ 準同型であって、逆写像も $\mathcal{C}$ 準同型であるものを $\mathcal{C}$ 同型という。一般に、f が全単射 $\mathcal{C}$ 準同型であれば、その逆写像も $\mathcal{C}$ 準同型であり従って同型となることが命題 2.1.13 の証明と同様にして確かめられる。 □

問題 2.21. 問題 2.8 において、

$$\mathrm{Exp} : (\mathbb{R}, +, 0) \to (\mathbb{C}, \times, 1)$$

は群準同型であり、群の準同型定理（準備段階）を用いることによって

$$(\mathbb{R}/\equiv, +, 0) \to (T, \times, 1)$$

なる群同型を与えることを示せ。

2.4.8 同値関係と部分群

群 G の部分集合が H が与えられたとき、次のような二項関係の定義をする。（この定義は逆元を用いており、G が群であることを利用していることを注意しておく。）

定義 2.4.35. $(G, \circ, e)$ を群とし、$H \subset G$ を G(の台集合) の部分集合とする。このとき、G(の台集合) の上の二項関係 $\sim_H^L$ を

$$\forall a, b \in G \quad a \sim_H^L b \Leftrightarrow a^{-1} \circ b \in H$$

で定義する。L は左 (left) の L である。

同様に、

$$\forall a, b \in G \quad a \sim_H^R b \Leftrightarrow a \circ b^{-1} \in H$$

で $\sim_H^R$ を定義する。

例 2.4.36. $H = \{e\}$ のとき、

$$a \sim_H^L b \Leftrightarrow a^{-1} \circ b \in \{e\} \Leftrightarrow a^{-1} \circ b = e \Leftrightarrow b = a.$$

よってこのときは $\sim_H^L$ は等号と一致する。

次の定理は、$\sim_H^L$ が同値関係であるということと、H が部分群であるということが同値であることを主張する。

定理 2.4.37. $(G, \circ, e)$ を群とし、H をその部分集合とする。$\sim_H^L$ が同値関係である必要十分条件は、H が部分群であることである。

証明. $\sim_H^L$ を単に $\sim$ であらわす。

- $\sim$ が [E2] を満たすことと、H が [S2] を満たすことが同値であること:

$$\forall a \quad a \sim a \Leftrightarrow a^{-1} \circ a \in H \Leftrightarrow e \in H.$$

- $\sim$ が [E3] を満たすことと H が [S3] を満たすことの同値性 :

  [E3] を満たせば

$$e \sim a \Leftrightarrow a \sim e.$$

  これを H の言葉でかけば

$$e^{-1} \circ a \in H \Leftrightarrow a^{-1} \circ e \in H.$$

  $e = e^{-1}$ より $a \in H \Rightarrow a^{-1} \in H$、従って H は [S3] を満たす。

  逆に H が [S3] を満たすならば、

$$a \sim b \Rightarrow a^{-1} \circ b \in H \overset{[\mathrm{E3}]}{\Rightarrow} (a^{-1} \circ b)^{-1} \in H$$

  ここで問題 2.19 を使うと

$$(a^{-1} \circ b)^{-1} = b^{-1} \circ (a^{-1})^{-1} = b^{-1} \circ a.$$

  これが H に入るのだから $b \sim a$。すなわち [E3] が言えた。

- $\sim$ に [E3] を仮定（または、同値である H に [S3] を仮定）した上での、$\sim$ が [E1] を満たすことと H が [S1] を満たすことの同値性 :

  $\sim$ が [E3] を満たすと仮定し、さらに [E1] を満たすとする。$a, b \in H$ とすると [S3] より $a^{-1} \in H$ よって $e \sim a^{-1}$。また $e \sim b$。[E3][E1] を使って $a^{-1} \sim b$。よって $(a^{-1})^{-1} \circ b \in H$、すなわち $a \circ b \in H$ で [S1] を満たす。

  逆に H が [S3][S1] を満たすとする。実は [S1] だけから [E1] が次のように従う。

$$a \sim b, b \sim c \Rightarrow a^{-1} \circ b, b^{-1} \circ c \in H \overset{[\mathrm{S1}]}{\Rightarrow} (a^{-1} \circ b) \circ (b^{-1} \circ c) \in H \Rightarrow a^{-1} \circ c \in H \Rightarrow a \sim c.$$

□

注意 2.4.38. 同様に、$\sim_H^R$ が同値関係となる必要十分条件も、$H < G$ となることである。

定義 2.4.39. G を群とし、$H < G$ をその部分群とする。定理 2.4.37 により、$\sim_H^L$ は G 上の同値関係である。この同値関係を H を法とする左**合同関係**という。

G(の台集合) をこの同値関係で割って得られる商集合を

$$G/H := G/\sim_H^L$$

であらわし、その一つ一つの元を G の H による**左剰余類** という。G/H を「G を右から H の作用で割って得られる商」、または「G の H による左剰余類集合」という。

同様に $\sim_H^R$ を H を法とする右合同関係といい、G のそれによる商集合を

$$H\backslash G := G/\sim_H^R$$

であらわし、G の H による**右剰余類**集合、あるいは G を左から H の作用で割って得られる集合という。

上の定義の状況で、$\sim_H^L$ に関して $a \in G$ の属する同値類 [a] は

$$[a] = \{g \in G | a \sim_H^L g\} = \{g \in G | a^{-1} \circ g \in H\} = \{g \in G | g \in a \circ H\} = a \circ H$$

である。ここで、$a \circ H$ は次に定義する集合である。

定義 2.4.40. $(G, \circ)$ をマグマとする。$S \subset G$, $a \in G$ のとき

$$a \circ S := \{a \circ s | s \in S\}$$

と定義する。同様に $b \in G$ に対し

$$S \circ b := \{s \circ b | s \in S\}$$

である。G が半群のときは

$$a \circ S \circ b := \{a \circ s \circ b | s \in S\}$$

と定義する。結合律により $a \circ s \circ b$ と書いてもまぎれがない。

またマグマの場合にもどって、$S, T \subset G$ のとき

$$S \circ T := \{s \circ t | s \in S,\ t \in T\}$$

と定義する。

混乱の恐れの少ない場合、$\circ$ はしばしば省略される。すなわち、$a \circ b$ の代わりに ab, $a \circ H \circ b$ の代わりに aHb, $S \circ T$ の代わりに ST と書かれる。

上の記法を用いれば、次を示したことになる。

命題 2.4.41. G を群、H をその部分群とする。$a \in G$ の属する $\sim_H^L$ に関する同値類、すなわち a の属する左剰余類は aH である。

$a \in G$ の属する $\sim_H^R$ に関する同値類、すなわち右剰余類は Ha である。

（特に、どちらの場合でも単位元 e の属する同値類は $[e] = H$ である。）

この命題に定理 1.3.11 を適用すると次を得る。

系 2.4.42. G を群、H をその部分群とする。任意の $a, b \in G$ に対し、

$$aH = bH \text{ または } aH \cap bH = \emptyset$$

のどちらか一つだけが成立する。G は aH の形の集合に分割される：

$$G = \coprod_{aH \in G/H} aH$$

注意 2.4.43.

$$G = \coprod_{aH \in G/H} aH$$

の式は少々わかりにくい。G/H の一つ一つの元は実は aH という形の集合である。$aH = a'H$ となるような a, a' もあるかも知れないが、そういうものは同じと思って、G/H の一つ一つの元 aH を並べると、G をきれいに交わりなく分割しているということである。

上は左剰余類の場合であるが、右剰余類でも同じことが言える。

問題 2.22.

$$a \sim_H^L b \Leftrightarrow b \in a \circ H$$

を示せ。

問題 2.23. $(\mathbb{Z}, +, 0)$ を整数のなす加法群とし、m を自然数とする。$H := m\mathbb{Z} := \{mx | x \in \mathbb{Z}\}$ を m の倍数の集合とする。（この記法は定義 2.4.40 で $\circ = \times$ の場合を用いている。）

1. H は部分群であることを示せ。
2. $\sim_H^L$ は、$\equiv_m$ を m を法とする合同関係 (定義 1.3.24) と一致することを示せ。
3. $$\mathbb{Z} = \coprod_{a=0,1,\ldots,m-1} (a + m\mathbb{Z})$$
   を示せ。（この記法は定義 2.4.40 で $\circ = +$ の場合を用いている。）

2.4.9　群の位数とラグランジュの定理

定義 2.4.44. (有限群, finite group)
$(G, \circ, e)$ を群とする。台集合 G が有限集合であるときこの群を**有限群** (finite group)、無限集合である場合**無限群** (infinite group) という。

注意 2.4.45. 注 1.1.1 で述べたように、無限にもいろいろな種類がある。それに応じて、可算無限群 (countably infinite group) 連続無限群 (continuum infinity group) などの定義がある。

定義 2.4.46. 台集合 G の元の数 $\#(G)$ を、群 G の**位数** (order) という。（G が無限集合の場合には、G の濃度を位数という。）

定理 2.4.47. (ラグランジュの定理)
G を群、H をその部分群とする。このとき

$$\#(G) = \#(G/H) \times \#(H)$$

が成立する。特に、$G/H, H$ の二つが有限集合ならば、G も有限集合。

証明.

$$G = \coprod_{aH \in G/H} aH$$

と分割されているわけだから、

$$\#(G) = \sum_{aH \in G/H} \#(aH)$$

である。ここで、

$$L_a : H \to aH, h \mapsto ah$$

と

$$L_{a^{-1}} : aH \to H, h \mapsto a^{-1}h$$

は互いに逆写像であり、一対一対応を与える。よって、$a \in G$ によらずに

$$\#(H) = \#(aH)$$

である。ということは、$\#(G)$ は $\#(G/H)$ 個の $\#(H)$ の和である、すなわち

$$\#(G) = \sum_{aH \in G/H} \#(aH) = \sum_{aH \in G/H} \#(H) = \#(G/H) \times \#(H).$$

□

系 2.4.48. G を有限群、H をその部分群とするとき、G の位数を H の位数は割り切る。

定義 2.4.49. G を群、$H < G$ を部分群とする。このとき、$\#(G/H)$ を G における H の**指数** (index) とよび、

$$[G : H]$$

であらわす。

定義 2.4.50. 一元集合 $\{x\}$ に対しては、二項演算は

$$x \circ x = x$$

と定義するほかはない。このとき $(\{x\}, \circ, x)$ は群である。このような群を**自明な群** (trivial group) という。
$(G, \circ, e)$ を群とすると、$(\{e\}, \circ, e)$ は部分群である。これと G 自身を合わせて、G の**自明な部分群**という。

問題 2.24. G を位数が素数であるような群とする。G の部分群は、自明な部分群のみであることを示せ。

2.4.10　指数法則と元の位数

半群に対して g^n $(n = 1, 2, \ldots)$ が定まり、モノイドに対しては g^0 も定まった (定理 2.3.26)。同様に、群に対して g^n $(n \in \mathbb{Z})$ が定義される。

定理 2.4.51. (群の指数法則)
$(G, \circ, e)$ を群とし、$g \in S$ を一つの元とする。整数 n に対し、

$$g^n = \begin{cases} g^n & (n > 0) \\ e & (n = 0) \\ (g^{-1})^{-n} & (n < 0) \end{cases}$$

と定義すると、次が成立する。

$$(g^n) \circ (g^m) = g^{n+m}.$$

証明は、$n, m \geq 0$ のときは定理 2.3.26 で示されている。その他の場合は、いろいろ場合分けしなくてはならない。たとえば $n > -m > 0$ の時は、

$$(g^n) \circ (g^m) = ((g^{n-1}) \circ g) \circ (g^{-1} \circ g^{m+1}) = (g^{n-1}) \circ g^{m+1} = \cdots = g^{n-(-m)}.$$

のこりの場合分けは読者に任せる。

系 2.4.52. $(G, \circ, e)$ を群とし、$g \in S$ を一つの元とする。このとき、

$$f : (\mathbb{Z}, +, 0) \to (G, \circ, e)$$

なる群準同型であって、$1_{\mathbb{Z}} \mapsto g$ となるものが唯一つ存在する。

証明. 存在するならば、逆元を逆元に移すこと (定義 2.4.17 の [HD]) より $f(-1) = f(1)^{-1} = g^{-1}$。よって $n > 0$ のとき

$$f(-n) = f((-1) + \cdots + (-1)) = f(-1) \circ \cdots \circ f(-1) = f(-1)^n = (g^{-1})^n = g^{-n}.$$

したがって存在すれば n の正負にかかわらず $f(n) = g^n$ となるしかない。これが群準同型であることは定理 2.4.51 に他ならない。 □

注意 2.4.53. このように、半群における $(\mathbb{N}, +)$, モノイドにおける $(\mathbb{N} \cup \{0\}, +, 0)$, 群における $(\mathbb{Z}, +, 0)$ は同じ役割を担っている。これらは、「1 元生成の自由対象」と呼ばれる。$(\mathbb{N}, +)$ は一元生成自由半群であり、$(\mathbb{Z}, +, 0)$ は一元生成自由群である。

問題 2.25. マグマにおいて、上の注に述べられたような性質をもつ対象（一元生成自由マグマと呼ぶべきもの）を記述せよ。

答は、$(((1,1),1),(1,1))$ のような「括弧のつけかた全体のなすマグマ」である。

問題 2.26. $(G, \circ, e)$ を群とし、$g \in G$ をその元とする。$m, n \in \mathbb{Z}$ に対して、

$$g^{mn} = (g^m)^n$$

を示せ。

定義 2.4.54. $(G, \circ, e)$ をモノイドとし、$g \in G$ をその元とする。g の位数 (order) $\mathrm{ord}(g)$ を、

$$\mathrm{ord}(g) := \min\{n \in \mathbb{N} | n \geq 1, g^n = e\}$$

で定義する。すなわち、g を何乗したら単位元に戻るか、その最小値を g の位数という。

g を何乗しても単位元にならないときは $\{n|n \geq 1, g^n = e\}$ は空集合であり、その最小値である $\mathrm{ord}(g)$ は無限大 ∞ と定義する。

定義 2.4.55. $(G, \circ, e)$ を群とし、$g \in G$ をその元とする。系 2.4.52 により与えられる $(\mathbb{Z}, +, 0)$ から $(G, \circ, e)$ への群準同型写像 $f : \mathbb{Z} \to G, \quad f(n) = g^n$ の像

$$\{g^n | n \in \mathbb{Z}\}$$

を g の生成する G の部分群といい、$< g >$ で表す。これが G の部分群になることは、「群準同型写像の像は部分群」という定理 2.4.33 の 1 から従う。

定理 2.4.56. G を群、$g \in G$ をその元とする。定義 2.4.55 と定理 2.4.33 より

$$\mathbb{Z}/\sim_f \to < g >$$

なる群同型が与えられる。

もし g の位数が無限大であるならば、$\sim_f$ は等号に一致し、

$$(\mathbb{Z}, +, 0) \to (< g >, \circ, e), \quad 1 \mapsto g$$

なる群同形が与えられる。

もし g の位数が有限の値 m ならば、$\sim_f$ は m を法とした合同関係 $\equiv \mod m$ と一致し、したがって

$$(\mathbb{Z}/m, +, 0) \to (< g >, \circ, e), \quad [1] \mapsto g$$

なる群同型が与えられる。

証明. 群準同型定理 2.4.33 の 2 から $\mathbb{Z}/\sim_f \to < g >$ が群同型であることは従う。

もしいま $\sim_f$ が等号関係と一致する、すなわち

$$x \sim_f x' \Leftrightarrow x = x'$$

であると仮定すると、$\sim_f$ による同値類は全て一点集合となり、$\mathbb{Z}/\sim_f = \mathbb{Z}$（注 1.3.3）となる。

もし、そうでないとすると

$$x \sim_f x' \text{ かつ } x \neq x'$$

なる整数 x, x' が存在する。$f(x) = f(x')$ より $g^x = g^{x'}$。対称性より $x > x'$ と仮定してよいので移項して $g^{x-x'} = e$。これにより、g の位数は有限である。これで前半が言えた。（位数が無限であれば $\sim_f$ は等号に一致。）

g の位数が有限値 m だとしよう。

$$x \equiv x' \mod m \Rightarrow x - x' = mt \Rightarrow g^{x-x'} = g^{mt} = (g^m)^t = e^t = e \Rightarrow g^x = g^{x'} \Rightarrow x \sim_f x'.$$

逆に、$x \sim_f x'$ と仮定すると、逆にたどって $g^{x-x'} = e$ まではわかる。対称性から $x - x' > 0$ としてよい。ここで、トリックという感じではあるが、

$$x - x' = mq + r, \quad 0 \leq r < m$$

なる整数 q, r をとる (問題 1.21)。すると

$$e = g^{x-x'} = (g^m)^q \circ g^r = e^q \circ g^r = g^r.$$

m は $g^m = e$ となる最小の $m \geq 1$ であったのに、$r < m$ でかつ $g^r = e$ である。これは矛盾しているのではなく、$r = 0$ であるということを意味している。(m は 1 以上にとったときの最小値であったから。)

すなわち $x - x'$ は m の倍数、すなわち

$$x \equiv x' \bmod m.$$

よって、$\sim_f$ と $\equiv \bmod m$ は一致する。 □

系 2.4.57. g の（元としての）位数は、$< g >$ の（群としての）位数に一致する。

証明. g の位数 m が有限のとき、$\mathbb{Z}/m \cong < g >$ であるから両辺の元の数は一致し、それは m である。g の位数が無限の時は、$\mathbb{Z} \cong < g >$ であるから $< g >$ の位数も無限である。 □

系 2.4.58. 有限群 $(G, \circ, e)$ の元 g の位数は有限であり、G の位数の約数となる。したがって

$$g^{\#(G)} = e$$

が成立する。

証明. ラグランジュの定理 2.4.47 を G と $H =< g >$ に対して適用すればよい。 □

ラグランジュの定理では、G が群であることがフルに使われている。モノイドではこのような性質は成り立たない。$(G, \circ, e)$ をモノイドとし、∞ を G の元ではない任意の記号とする。$\circ$ を

$$\forall g \in G \quad g \circ \infty = \infty \circ g = \infty$$

で ∞ にも拡張すれば、$(G \cup \{\infty\}, \circ, e)$ はモノイドであり、G を部分モノイドとして含む。したがって、「G の位数を 1 増やせる」ので、モノイドの定理として G の位数とその元の位数の間に整除関係が示せることはない。

定義 2.4.59. $(\mathbb{Z}, +, 0)$ または $(\mathbb{Z}/m, +, 0)$ に同型な群を巡回群 (cyclic group) という。

これらの群は、1 または [1] により生成される。定理 2.4.56 によれば、群 G の一元 g で生成される部分群 $< g >$ は巡回群である。

問題 2.27. 群 $(\mathbb{Z}, +, 0)$ の $+$ とコンパチブルな $\mathbb{Z}$ 上の同値関係 $\sim$ に対し、ある 0 以上の整数 m が存在して $\sim$ は $\equiv \bmod m$ に一致することを示せ。

$1/2 = 0.5$	有限、非循環部 1
$1/3 = 0.3333\cdots$	周期 1
$1/4 = 0.25$	有限、非循環部 2
$1/5 = 0.2$	有限、非循環部 1
$1/6 = 0.16666\cdots$	周期 1 非循環部 1
$1/7 = 0.142857142857\cdots$	周期 6
$1/8 = 0.125$	有限、非循環部 3
$1/9 = 0.111111111\cdots$	周期 1
$1/10 = 0.1$	有限、非循環部 1
$1/11 = 0.0101010\cdots$	周期 2
$1/12 = 0.08333\cdots$	周期 1 非循環部 2
$1/13 = 0.076923076923\cdots$	周期 6
$1/14 = 0.0714285714285\cdots$	周期 6 非循環部 1
$1/15 = 0.06666\cdots$	周期 1 非循環部 1
$1/16 = 0.0625$	有限、非循環部 4
$1/17 = 0.058823529411764$ $7058823529\cdots$	周期 16

図 2.1: $1/n$ の少数展開

2.4.11 循環小数

群の公理は、何か自明なものである。なぜ、こんな砂を噛むような抽象的なものを扱わなくてはならないのか。というのが、私が最初に群の公理に触れたときの思いであった。

この節では、「循環小数の周期」という小学校算数に現れる概念が群と密接にかかわっていることを見る。

$1/n$ の形の有理数を小数展開すると、有限小数になるか循環小数になるか、どちらかであることが知られている。実際に計算してみると、図 2.1 のようになる。ここに、「有限」と書いたのは有限小数となるとき、「周期」と書いたのはどこからか周期的になるときで、その周期の長さをその後に書いた。「非循環部」と書いたのは、小数以下最初の方に循環しない部分があるときの、その長さを表す。例えば $1/12$ では、小数部は $083333\cdots$ なので、非循環部は 08 でありその長さは 2 で、周期は 1 である。$1/16 = 0.0625$ では、0625 を非循環部とみなしその長さは 4 とする。

もう少し周期の長い例をあげると、$1/23$ は周期 22 で循環し、$1/113$ は周期 112 で循環する。

問題 2.28. 上の表を見て、n とその小数展開の様子との関係についてさまざまな予想を立てよ。

特に、n が 2 でも 5 でもない素数の時には、$1/n$ は非循環部分なく循環し、その周期は $n-1$ を割りきることが見える。

この節では、この事実を証明してみる。その際、群の概念が自然にあらわれる。

余録

例えば、次のような性質がなりたつ。

命題 2.4.60. $1/n$ の小数部分に対して次が成り立つ。

1. 周期は $n-1$ 以下。
2. n が素数以外の時には、周期は $n-1$ になることはない。
3. n が素数の時には、周期は $n-1$ を割る。（この「割る」というのは「割りきる」という意味である。）
4. 周期は $\varphi(n)$ を割る。ここに、$\varphi(n)$ はオイラーの関数と呼ばれる関数で、$0, 1, 2, \ldots, n-1$ のうちで n と互いに素な物の個数をあらわす。(後述、系 2.4.68 を参照。ここから 1, 2, 3 は容易に従う。)
5. 有限小数になるのは、n が $2^s \times 5^t$ (s,t は 0 以上の整数) のとき、かつその時に限る。
6. 非循環部分の長さは、次のようにして求まる。n を 2 と 5 で割れるだけ割って

$$n = 2^s \times 5^t \times m,$$

m は 2 でも 5 でも割れない、という形にする。非循環部の長さは、s, t の大きいほう。

2.4.12　可換群 $\mathbb{Z}/n$ と $(\mathbb{Z}/n)^\times$

1/7 の小数展開を筆算で行うと、次のようになる。
1/7 の筆算 (図 2.2) を上の方から見ていくと、次のようになっている。

$$\begin{array}{l} 1 \times 10 \div 7 = 1 \quad \text{余り } 3 \\ 3 \times 10 \div 7 = 4 \quad \text{余り } 2 \\ 2 \times 10 \div 7 = 2 \quad \text{余り } 6 \\ 6 \times 10 \div 7 = 8 \quad \text{余り } 4 \\ 4 \times 10 \div 7 = 5 \quad \text{余り } 5 \\ 5 \times 10 \div 7 = 7 \quad \text{余り } 1 \\ 1 \times 10 \div 7 = 1 \quad \text{余り } 3 \\ \vdots \end{array} \tag{2.2}$$

上の繰り返しの、左端にあらわれる数列 $x_1 = 1, x_2 = 3, x_3 = 2, \ldots$ の部分を漸化式の言葉で書くと、次のようにあらわせる。

$$x_1 = 1, \quad x_i := (x_{i-1} \times 10) \bmod 7 \quad (i = 2, 3, 4, \ldots) \tag{2.3}$$

ここで、記号 $a \bmod b$ は「a を b で割った余り」をあらわす。この数列は、

$$(\mathbb{Z}/7, \times, [1])$$

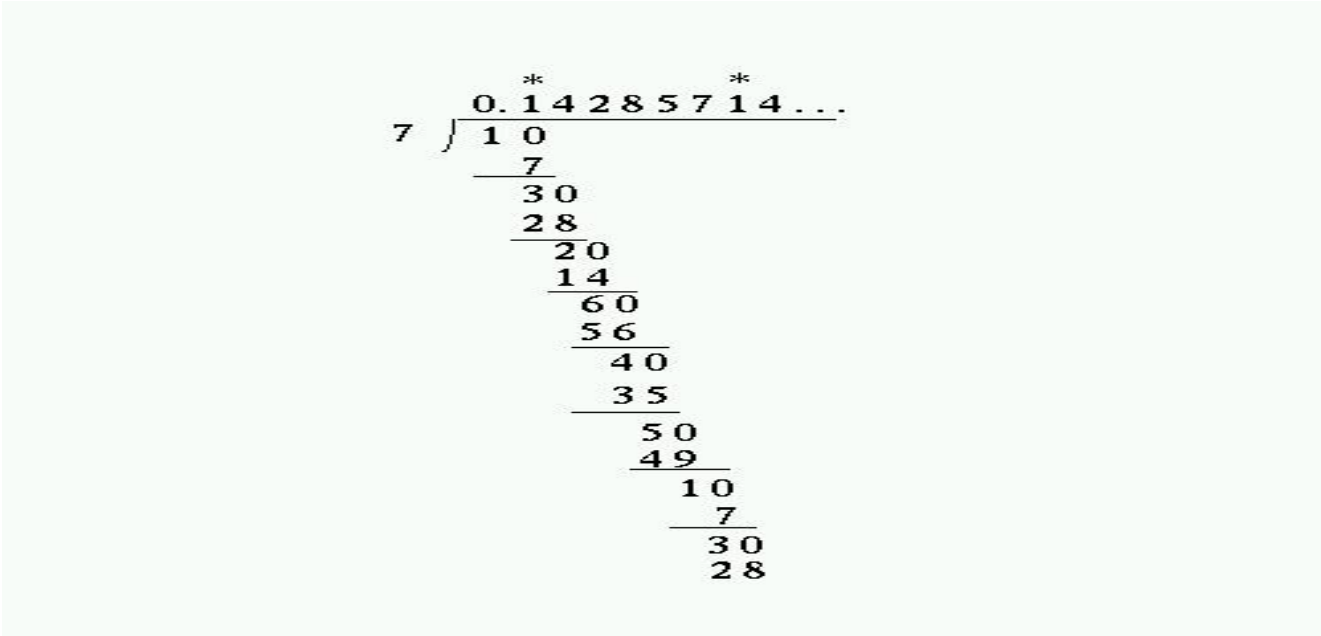

図 2.2: 1/7 の 10 進小数展開の筆算

なるモノイドにおいて、漸化式

$$x_1 = [1], x_m = x_{m-1} \times [10]$$

を解いて得られる数列にほかならない。従って

$$x_1 = [1], x_2 = [1] \times [10] = [10], x_3 = x_2 \times [10] = [10]^2, \ldots, x_m = [10]^{m-1}, \ldots$$

となる。

より一般に、$1/n$ の小数展開には

$$x_1 = 1, \quad x_i = (x_{i-1} \times 10) \bmod n \quad (i = 2, 3, 4, \ldots) \tag{2.4}$$

の計算があらわれる。これはモノイド $(\mathbb{Z}/n, \times, 1)$ において

$$x_i = [10]^{i-1} \quad (i = 1, 2, \ldots)$$

を計算していることに他ならない。

そして、小数展開の i 桁目を a_i とする (すなわち $1/n = 0.a_1a_2a_3\cdots$ とおく) と

$$a_i = (x_i \times 10) \div n \text{ の商} \quad (i = 1, 2, 3, \ldots)$$

である。すなわち、a_i は x_i から決まる。また逆に、a_i から x_i は

$$\begin{aligned} x_i &= 10^{i-1} \times (1 - 0.a_1a_2\cdots a_{i-1} \times n) \\ &= \{10^{i-1} \times (1/n - 0.a_1a_2\cdots a_{i-1})\} \times n \\ &= \{0.a_{i+1}a_{i+2}\cdots\} \times n \end{aligned}$$

で求まる。i を増やしていったときの最後の式に現れる $\{\}$ の中味の循環のしかたは、a_i の循環のしかたと同じである。このように x_i から a_i が決まり、逆に a_i から x_i が決まるので、余りの数列 x_i と小数点以下の桁の数列 a_i の振るまいは同じである。例えば、周期は同じだし、非循環部分の長さも同じである。

いまもし [10] が可逆元の作る群 (命題 2.4.9 参照) $(\mathbb{Z}/n^\times, \times, 1)$ に入っていたとすると、[10] の位数は有限値 s となる。この位数が数列 x_m の周期であり、非循環部なく周期的になることが定理 2.4.56 の帰結である。($e = g^0, g^1, g^2, \ldots, g^{s-1}, g^s = e, \ldots$ と循環する。)

これにより、次の命題が言えた。

命題 2.4.61. n を自然数とする。$[10] \in \mathbb{Z}/n$ が積に関して可逆であるとき、$1/n$ の少数展開は純周期的になりその周期は [10] の $\mathbb{Z}/n^\times$ における（積に関する）位数に一致する。

系 2.4.58 を使えば次が導かれる。

系 2.4.62. 上の条件のもとで、周期は $\mathbb{Z}/n^\times$ の位数の約数となる。

次の定理の証明には、初等整数論が必要となる。

定理 2.4.63. $(\mathbb{Z}/n)^\times = \{m \in \mathbb{Z}/n \mid m \text{ と } n \text{ は互いに素 }\}$

0 と n の最大公約数は n であり、0 と $n \geq 2$ は互いに素でないことに注意しておく。

証明.

$\subset$ を言う。（といういいかたをしたら、「$(\mathbb{Z}/n)^\times \subset \{m \in \mathbb{Z}/n | m \text{ と } n \text{ は互いに素 }\}$ を証明します」という意味である。）$m \in (\mathbb{Z}/n)^\times$ をとってこよう。m と n が互いに素であることを示せば良い。

背理法を用いる。もし、m と n が互いに素でなかったとすると m と n には公約数 $d > 1$ が存在して $m = m_0 d$, $n = n_0 d$ となる。m の可逆性から、ある $a \in \mathbb{Z}/n$ が存在して $a \cdot m = 1$ が $\mathbb{Z}/n$ で成り立つ。a を整数と思うと、$(a \cdot m) \bmod n = 1$ ということである。これは、ある整数 b が存在して

$$am + bn = 1$$

となることを意味している。(am を n で割った余りが 1 だから、$am - 1$ は n で割れる。$am - 1 = qn$ と書いたとき、$-q$ を b とすれば良い。)

ここで、$am + bn$ は d で割りきれるのに、1 は $d > 1$ で割りきれないから矛盾である。実際、$m = m_0 d$ かつ $n = n_0 d$ なので $am + bn = am_0 d + bn_0 d = (am_0 + bn_0)d$ であり d の倍数となる。

$\supset$ を言う。右辺から元をとってくると、$m \in \mathbb{Z}/n$ であって n と互いに素である。次の定理 2.4.64 によれば

$$am + bn = 1$$

をみたす整数 a, b が存在する。このとき

$$am = (-b)n + 1$$

より

$$am \bmod n = 1$$

そこで

$$a' := a \bmod n$$

とおくと $\mathbb{Z}/n$ の元として

$$a'm = ma' = 1$$

だからたしかに m は可逆で、$m \in (\mathbb{Z}/n)^\times$。

□

定理 2.4.64. m, n を整数とし、その最大公約数を d をすると、

$$\{am + bn | a, b \in \mathbb{Z}\} = \{cd | c \in \mathbb{Z}\}$$

が成り立つ。

系 2.4.65. 上で $d = 1$、すなわち m, n が互いに素とする。すると、$am + bn$ の形に表せる整数は、全ての整数である。特に

$$am + bn = 1$$

となるような a, b がある。

証明. $am + bn$ の形にかける整数は、全て d の倍数である。これで $\subset$ は言えた。

$\supset$ をいう。$m = n = 0$ ではないとする。$am + bn$ の形にかける正の整数のうち、最小のものをとって $e = a_0 m + b_0 n$ とおく。e は d の倍数であるから $e \geq d$。e が m, n の公約数であることを言えば、d は最大公約数なので $d \geq e$。よって $d = e$ となる。$a_0 m + b_0 n = d$ となったので、$(ca_0)m + (cb_0)n = cd$。よって $\supset$ はいえる。

e が m, n の公約数であることを言えば証明は終わる。いま、m を e で整除して

$$m = qe + r, \quad 0 \leq r \leq e - 1$$

とできる。すると、

$$r = m - qe = m - q(a_0 m + b_0 n) = (1 - qa_0)m + (-qb_0)n$$

となり、r も $a'm + b'n$ の形に表せる。e は、このようにあらわせる正の整数の中で最小のものであったのに、$0 \leq r \leq e - 1$ である。$r > 0$ だとしたら、e の代わりに r がとれたはずなので、矛盾である。すなわち、$r = 0$ 以外にありえない。これは m が e で割りきれることを示している。

同様に、m と n の役目をいれかえると n が e で割りきれることがわかる。よって e は m, n の公約数である。 □

注意 2.4.66. 上の定理は、単項イデアル整域の定理としてとらえるのが良い（§4.7.3）。

注意 2.4.67. 上の定理の証明には、小さな問題がある。$n = 0$ や $m = 0$ のとき、その最大公約数はどう定義するべきか？$n = m = 0$ の時はどうするか？

通常は、0 と m の最大公約数は m とする。よって、0 と 0 の最大公約数は 0 である。$m = n = 0$ の時には上の証明は使えない（どこで破綻するか？）が、結論は正しい（各自確かめよ）。

系 2.4.68. $\#(\mathbb{Z}/n)^\times = \varphi(n)$. ここに、$\varphi(n)$ は $0, 1, 2, \ldots, n-1$ のうちで n と互いに素なものの個数で、**オイラーの関数**と呼ばれる。(命題 2.4.60 にもあらわれている。)

特に n が素数ならば

$$(\mathbb{Z}/n)^\times = \{1, 2, \cdots, n-1\} \subset \mathbb{Z}/n$$

で $\varphi(n) = n - 1$。

これに命題 2.4.61 とその系を使う。条件 $[10] \in (\mathbb{Z}/n)^\times$ は、10 と n が互いに素である、すなわち n が素因数として 2 も 5 も持たないということである。この条件のもとで、$[10]$ の位数は $\varphi(n)$ の約数となり $1/n$ の小数展開はこの位数を周期として循環する。これで n と 10 が互いに素であるときの、命題 2.4.60 が示された。

問題 2.29. （やや難）

命題 2.4.60 を証明せよ。

2.4.13　正規部分群と準同型定理

群が半群やモノイドに比べて重要な理由はいくつかある。そのうちの一つは、上で見たように群においては「元の位数」というそれぞれの元の性質が、「群全体の位数」という全体の性質と密接に関連していることが上げられる。

他の理由の一つに、「二項演算とコンパチブルな同値関係」というものが「正規部分群」という扱いやすい概念と本質的に同じ (注 1.3.3) であるということが挙げられる。

まず、群準同型

$$f : (G_1, \circ_1, e_1) \to (G_2, \circ_2, e_2)$$

が与えられたとき、$\sim_f$ がどのように表せるかを見よう。

定義 2.4.69. $(G_1, \circ_1, e_1), (G_2, \circ_2, e_2)$ を群とし、$f : G_1 \to G_2$ を群準同型とする。f による e_2 の逆像を f の**核** (**kernel**) といい $\mathrm{Ker} f$ と書く。すなわち、

$$\mathrm{Ker} f := f^{-1}(e_2) = \{x \in G_1 | f(x) = e_2\}.$$

命題 2.4.70. 上の状況で、$a \sim_f b \Leftrightarrow a \sim^L_{\mathrm{Ker} f} b$.

証明.

$$a \sim_f b \Leftrightarrow f(a) = f(b) \Leftrightarrow f(a)^{-1} f(b) = e_2 \Leftrightarrow f(a^{-1}b) = e_2 \Leftrightarrow a^{-1}b \in \mathrm{Ker} f.$$

□

系 2.4.71. 上で f が単射である必要十分条件は、$\mathrm{Ker} f = \{e\}$ であることである。

さて、一般に群準同型の核は部分群となるが、実は正規部分群と呼ばれる特殊な部分群となる。

定義 2.4.72. 群 $(G, \circ, e)$ の部分群 H が**正規部分群** (normal subgroup) であるとは、

$$\forall a \in G \quad aHa^{-1} = H$$

であること。

注意 2.4.73. 上の定義を

$$\forall a \in G \quad aHa^{-1} \subset H$$

としても同値である。なぜなら、$aHa^{-1} \subset H$ であるが、このとき a は任意であるから a の代わりに a^{-1} をとると

$$a^{-1}Ha \subset H$$

となる。左から a を掛けて右から a^{-1} を掛けると

$$H \subset aHa^{-1}$$

となり、最初の包含関係と合わせて

$$H = aHa^{-1}$$

が言えるからである。

命題 2.4.74. $f : G_1 \to G_2$ を群準同型とすると、$\mathrm{Ker}f$ は G_1 の正規部分群となる。

証明. [S1]:

$$a, b \in \mathrm{Ker}f \Rightarrow f(a \circ_1 b) = f(a) \circ_2 f(b) = e_2 \circ_2 e_2 = e_2 \Rightarrow a \circ_1 b \in \mathrm{Ker}f.$$

[S2]: $e_1 \in \mathrm{Ker}f$ は [HC]$f(e_1) = e_2$ から従う。
[S3]:

$$a \in \mathrm{Ker}f \Rightarrow f(a^{-1}) = f(a)^{-1} = e_2^{-1} = e_2$$

従って $a^{-1} \in \mathrm{Ker}f$.

以上より部分群。また、任意に $g \in \mathrm{Ker}f$ および $a \in G_1$ を取ったとき、

$$f(a \circ g \circ a^{-1}) = f(a) \circ f(g) \circ f(a)^{-1} = f(a) \circ e_2 \circ f(a)^{-1} = e_2.$$

よって $aga^{-1} \in \mathrm{Ker}f$, すなわち

$$a(\mathrm{Ker}f)a^{-1} \subset \mathrm{Ker}f.$$

上の注意より $\mathrm{Ker}f$ は正規部分群となる。 □

群 $(G, \circ, e)$ に対し、$\sim$ がその台集合上の演算 $\circ$ とコンパチブルな同値関係であるとする。すると、定理 2.4.24 により商群への商準同型

$$q : G \to G/\sim$$

が定義され、$\sim = \sim_q$ である。$\mathrm{Ker}q = [e]$ であるから、命題 2.4.70 より次の定理の前半が言える。

定理 2.4.75. $(G, \circ, e)$ を群、$\sim$ を $\circ$ とコンパチブルな同値関係とすると、$H := [e]$ は G の正規部分群であり、$\sim$ と $\sim_H^L$ は一致する。従って

$$G/\sim = G/H$$

となる。

逆に、H が G の正規部分群であれば、$\sim_H^L$ は $\circ$ とコンパチブルな同値関係であり、

$$G/\sim_H^L = G/H$$

は群となり、$q : G \to G/H$ は群準同型写像となる。

証明. 後半の、H が正規部分群のとき、$\sim_H^L$ と $\circ$ がコンパチブルなことのみ示せばよい。
$a \sim_H^L a'$ かつ $b \sim_H^L b'$ ならば、

$$(ab)^{-1}(a'b') = b^{-1}(a^{-1}a')b' = (b^{-1}b')(b'^{-1}a^{-1}a'b') \in H \circ b'Hb'^{-1} \subset H$$

より $ab \sim_H^L a'b'$、ゆえに $\circ$ と $\sim_H^L$ はコンパチブルとなる。 □

以上により、商群の定理 2.4.24、well-definedness の定理 2.4.31 および群の準同型定理 2.4.33 は次のように言い換えられる。

定理 2.4.76. $(G, \circ, e_G)$ を群とし、N を G の正規部分群とすると、商写像

$$q : G \to G/N$$

が群準同型となるような二項演算 $\bar{\circ}$ と 0 項演算 $\bar{e_G}$ と単項演算 $()^{-1}$ が G/N に定義される。
このとき、$(G/N, \bar{\circ}, \bar{e_G})$ を G の N による**商群**といい、q を商準同型と言う。

定理 2.4.77. $(X, \circ_X, e_X)$ を群とし、N を X の正規部分群とする。$q : X \to X/N$ を商準同型とし、任意の群 $(Y, \circ_Y, e_Y)$ と任意の群準同型 $f : X \to Y$ を考える。
群準同型 $h : X/N \to Y$ であって、

$$f = h \circ q$$

なる性質をもつものが存在する必要十分条件は、

$$N \subset \mathrm{Ker} f$$

となることである。このとき、h はただ一つに決まる（しばしば $\bar{f}$ で表される。）
この状況を $\bar{f}$ が **well-defined** であるという。

証明. 定理 2.4.31 からのただちの帰結である。

$$a \sim_N^L b \Rightarrow f(a) = f(b)$$

なる条件が、

$$a^{-1}b \in N \Rightarrow f(a^{-1}b) = e$$

と言い換えられ、$N \subset \mathrm{Ker} f$ と言い換えられるからである。 □

定理 2.4.78. (**群の準同型定理**) $(X, \circ_X, e_X)$、$(Y, \circ_Y, e_Y)$ を群とし、$f : X \to Y$ なる群準同型が与えられたとする。$f(X) \subset Y$ で f による X の像を表す。このとき、

1. $f(X)$ は Y の部分群である。
2. $N := \mathrm{Ker} f$ は X の正規部分群で、$\sim_N^L$ は $\circ$ とコンパチブルな同値関係である。
3. f が

$$X \xrightarrow{q} X/N \xrightarrow{\bar{f}} Y$$

なる合成となるような $\bar{f}$、すなわち

$$f = \bar{f} \circ q$$

なる $\bar{f}$ がただ一つ存在する。そして、その終集合を $f(X)$ に制限して得られる

$$\bar{f} : X/N \to f(X)$$

は群同型となる。

通常、この定理が群準同型定理と呼ばれている。そのため、定理 2.4.33 には「準備段階」との注意書きを入れた。

N が G の正規部分群であることを

$$N \triangleleft G$$

であらわす。

問題 2.30. 問題 2.21 において、

$$\mathrm{Exp} : (\mathbb{R}, +, 0) \to (\mathbb{C}^\times, \times, 1)$$

に群準同型定理 2.4.78 を用いることで、

$$(\mathbb{R}/\mathbb{Z}, +, 0) \to (T, \times, 1)$$

なる群同型を与えよ。

問題 2.31. 絶対値をとるという写像

$$f : (\mathbb{C}^\times, \times, 1) \to (\mathbb{R}^\times, \times, 1), \quad f(z) = |z|$$

が群準同型であることを示し、群準同型定理を用いて

$$\mathbb{C}^\times/T \to \mathbb{R}_{>0}$$

なる群同型を構成せよ。ここに $\mathbb{R}_{>0}$ は正の実数が積に関してなす群をあらわす。

問題 2.32. 複素数 $z \in \mathbb{C}^\times$ に対して $\frac{z}{|z|}$ を対応させることで、$\mathbb{C}^\times/\mathbb{R}_{>0} \to T$ なる群同型を構成せよ。

問題 2.33. K を実数の集合 $\mathbb{R}$ とする（次節で定義する一般の可換環でもよい）。行列式 $A \mapsto \det(A)$ が

$$(GL_n(K), \times, I_n) \to (K^\times, \times, 1)$$

なる群準同型であることを示せ。

行列式が 1 であるような行列のなす $GL_n(K)$ の部分集合を $SL_n(K)$ (特殊線形群, special linear group) で表す。$SL_n(K)$ が $GL_n(K)$ の正規部分群であることを示し、$GL_n(K)/SL_n(K)$ がどんな群と同型になるか記述せよ。

2.5 環、体

環と体の定義だけ、先走りして簡単に述べておく。

定義 2.5.1. 環 (英語 ring) R とは、集合 R とその上の二つの二項演算 $+, \cdot$ の組 $(R, +, \cdot)$ であって、次の三つの公理（環の公理という。）を満たすもの。

R1 $(R, +)$ は加法群をなす。この単位元を $0 \in R$ であらわす。

R2 $(R, \cdot)$ は半群をなす。

R3 (分配法則) 任意の $a, b, c \in R$ に対して $(a+b)\cdot c = (a\cdot c)+(b\cdot c)$, $a\cdot(b+c) = (a\cdot b)+(a\cdot c)$ が成立する。

さらに、次の条件

R2' (積の単位元と呼ばれる)$1 \in R$ が存在し、$(R, \cdot, 1)$ が 1 を単位元とするモノイドとなる

を満たすとき、$(R, +, 0, \cdot, 1)$ を**単位的環**（英 ring with unit）という。**単位環** (unital ring) ともいう。

さらに、条件

R4 (積の可換性）$(R, \cdot)$ が可換な半群である、すなわち任意の $a, b \in R$ に対して $a \cdot b = b \cdot a$

が成り立つとき、R を**可換環** (commutative ring) という。可換環でない環を**非可換環**という。

$(R, +, \cdot)$ が環（従って [R1]-[R3] を満たす）であるとき、さらに

F モノイド $(R, \cdot, 1)$ において、 0 の補集合 $R - \{0\}$ は積について群をなす

を満たすとき、$(R, +, \cdot)$ を斜体 (skew field) という。積が可換であるような (すなわち [R4] を満たすような) 斜体を**可換体** (commutative field)、または単に**体** (field, 独 Körper) という。

体を文字 K で表すことが多い。これは上記のようにドイツ語の「Körper からだ」に由来する。「四則演算ができる」ということと「手足 4 本がある」を結び付けたらしい。しかし、英語では field という「からだ」とは無関係な名前が付いた。

例 2.5.2. $\mathbb{Z}/n$ は可換環となる。$\mathbb{Z}$ は加法群であり、$\mathbb{Z}/n$ には加法 $\bar{+}$ が定義されて加法群になる (例 2.4.8)。$(\mathbb{Z}/n, \bar{\times}, [1])$ がモノイドであることも例 2.3.22 で見た。分配法則 [R3] を示す。言いたいことは

$$([a]\bar{+}[b])\bar{\cdot}[c] = ([a]\bar{\cdot}[c]) + ([b]\bar{\cdot}[c])$$

であるが、左辺は

$$([a+b])\bar{\cdot}[c] = [(a+b)\cdot c] = [a\cdot c + b\cdot c] = [a\cdot c]\bar{+}[b\cdot c] = [a]\bar{\cdot}[c]\bar{+}[b]\bar{\cdot}[c]$$

で右辺に一致する。($q : a \mapsto [a]$ が二つの演算を保つことを何度も用いた。)

積の可換性 [R4] を示すのは、読者に任せる。

$\mathbb{Z}/n$ における $\bar{+}, \bar{\times}, [0], [1]$ は、通常単に $+, \times, 0, 1$ と書かれる。

命題 2.5.3. n を自然数とする。可換環 $(\mathbb{Z}/n, +, \times)$ が可換体となる必要十分条件は、n が素数であることである。

証明. 体となるには、0 を除いた元の集合が群となることが必要かつ十分である。$n=1$ のときは、0 を除いた $\mathbb{Z}/n$ の元の集合は空集合となり、単位元が存在しないので体でない。$n \geq 2$ とする。系 2.4.68 によれば、$\mathbb{Z}/n$ における積の非可逆元は、$0, 1, \ldots, n-1$ のうちで n と互いに素でないものである。n が素数ならばそれは 0 のみであり、n が素数でなければ 0 以外にも存在する。これにより、非可逆元が 0 だけである必要十分条件は、n が素数であることである。 □

注意 2.5.4. 環の理論における、イデアルと剰余環の一般論を使うと、$\mathbb{Z}/n$ が環であることの証明はより透明になる。これはあとで触れる。

群・環・体は 1 次方程式を解くために自然にあらわれたとも言える。$(\mathbb{N}, +)$ は半群だがモノイドでない。0 が発見されて $(\mathbb{N} \cup \{0\}, +)$ となって、モノイドになった。負の数が発見されて $(\mathbb{Z}, +)$ は可換群となった。

このとき、$(\mathbb{N}, +, \cdot)$ は補われて $(\mathbb{Z}, +, \cdot)$ なる可換環となった。しかし、これはまだ体ではない。0 以外の元が、積に関する逆元を持たなければ体ではないのである。

そこで、分数の発明により、$(\mathbb{Q}, +, \cdot)$ は体となった。この体を有理数体 (rational number field) という。$(\mathbb{R}, +, \cdot)$ も体で、実数体 (real number field) と呼ばれる。$(\mathbb{C}, +, \cdot)$ も体で、複素数体 (complex number field) と呼ばれる。

一方、抽象的概念としての「群」は負の数の発見よりずっとあとに、ガロアにより 19 世紀に与えられた。通常、「群の発明」と言えばこちらを指す。

2.6 直積

集合、マグマ、半群、モノイド、群が与えられたとき、それをもとに新たにそういった対象を構成する方法がいろいろある。最も代表的なものが直積である。

定義 2.6.1. G_1, G_2 をマグマ (または半群、モノイド、群) とするとき、それらの**直積**と呼ばれ、$G_1 \times G_2$ と記されるマグマ（または半群、モノイド、群）が次のように構成される。

1. 台集合は、G_1 の台集合と G_2 の台集合の集合としての直積。すなわち、
$$G_1 \times G_2 = \{(g_1, g_2) | g_1 \in G_1, g_2 \in G_2\}$$
2. 二項演算は、成分毎に行う。すなわち
$$(g_1, g_2) \circ (g_1', g_2') := (g_1 \circ_1 g_1', g_2 \circ_2 g_2').$$
3. モノイドの場合、直積の単位元は G_1, G_2 の単位元を並べたもの (e_1, e_2)。
4. 直積モノイドにおいて (g_1, g_2) が可逆である必要十分条件は、g_1 が G_1 で、g_2 が G_2 でそれぞれ可逆であること。このとき、逆元は (g_1^{-1}, g_2^{-1}) で与えられる。

   特に、群の直積は群になる。

三つの群 G_1, G_2, G_3 が与えられたとき、$G_1 \times G_2 \times G_3$ も同様に定義される。

$$G_1 \times G_2 \times G_3 \cong (G_1 \times G_2) \times G_3 \cong G_1 \times (G_2 \times G_3)$$

となる。(≅ は群の同型。)

無限個の直積も考えられる。Λ を集合とし、$(G_\lambda)_{\lambda\in\Lambda}$ を群 (あるいはマグマ、半群、モノイド) の族とする。それらの直積

$$\prod_{\lambda\in\Lambda} G_\lambda$$

とは、台集合としては G_λ の台集合の直積をとり、演算を成分毎で定義して得られる。すなわち、元は $(g_\lambda)_{\lambda\in\Lambda}$ なる列であり (全ての $\lambda \in \Lambda$ に対して $g_\lambda \in G_\lambda$ を一つずつ選んで並べたもの)、二項演算は

$$(g_\lambda)_{\lambda\in\Lambda} \circ (g'_\lambda)_{\lambda\in\Lambda} := (g_\lambda \circ g'_\lambda)_{\lambda\in\Lambda}$$

で与えられる。

G_1, G_2 のことが十分わかれば、$G_1 \times G_2$ のことも良く分かったと見なせる。このため、未知の群 G を既知の群 $G_1, G_2, \ldots, G_n$ の直積と同一視する（同型を探す）ことが重要となる。

例えば、G_1 における元の位数、G_2 における元の位数から、その直積における元の位数は次のようにしてもとまる。

命題 2.6.2. G_1, G_2 を群とする。このとき、$(g_1, g_2) \in G_1 \times G_2$ の位数は、g_1 の位数と g_2 の位数の最小公倍数となる。

証明.

$$(g_1, g_2)^m = e \Leftrightarrow (g_1^m, g_2^m) = (e_1, e_2) \Leftrightarrow g_1^m = e_1, g_2^m = e_2.$$

この最後の条件は m が g_1 の位数で割りきれ，かつ m が g_2 の位数で割り切れるということである。(ただし、無限大で割りきれる数は無限大のみとする。) このような最小の m が定義より (g_1, g_2) の位数だが、それは g_1, g_2 の位数の最小公倍数にほかならない。 □

では、与えられた G に対し、$G \cong G_1 \times G_2$ となるような G_1, G_2 があるとしよう。それを見つけるにはどうすればよいか。まず必要条件として、G_1 は G のある部分群と同型になることが次のようにしてわかる。$\iota_1 : G_1 \to G_1 \times G_2, \quad g_1 \mapsto (g_1, g_2)$ は単射群準同型である。よって G_1 と $\iota_1(G_1)$ は同型。$\varphi : G_1 \times G_2 \to G$ を群同型とすれば、$\varphi(\iota_1(G_1)) < G$ は G_1 と同型な G の部分群である。同様に、$\iota_2 : G_2 \to G_1 \times G_2$ なる単射群準同型があり、$\varphi(\iota_2(G_2)) < G$ は G_2 と同型な G の部分群である。従って，$G \cong G_1 \times G_2$ となるための一つの必要条件として，G に G_1 と同型な部分群 $\varphi(\iota_1(G_1))$ と G_2 に同型な部分群 $\varphi(\iota_2(G_2))$ がとれることがあげられる。

ここで逆に、$G_1, G_2 < G$ なる二つの部分群が与えられたとき，写像 $(g_1, g_2) \mapsto g_1 \circ g_2$ が

$$G_1 \times G_2 \cong G$$

なる群同型を与えるための条件を考えよう。

命題 2.6.3. $G_1, G_2 < G$ が与えられたとき、

$$h : G_1 \times G_2 \to G, \quad (g_1, g_2) \mapsto g_1 \circ g_2$$

が同型となる必要十分条件は、

1. G_1 の元と G_2 の元は可換
2. $G_1 \cap G_2 = \{e\}$
3. G の任意の元が $g_1 \circ g_2$ の形（$g_1 \in G_1, g_2 \in G_2$）と書ける

の 3 条件を満たすことである。

証明. 必要性は次の通り。$h : G_1 \times G_2 \to G$ が同型であるとする。$g_1 \in G_1$, $g_2 \in G_2$ に対し、$G_1 \times G_2$ において

$$(g_1, e_2) \circ (e_1, g_2) = (g_1, g_2) = (e_1, g_2) \circ (g_1, e_2)$$

である。これを h によって G に送ると、h の準同型性から

$$h((g_1, e_2)) \circ h((e_1, g_2)) = h((e_1, g_2)) \circ h((g_1, e_2))$$

だが、これは $g_1 \circ g_2 = g_2 \circ g_1$ に他ならない ($e_1 = e_2 = e_G$ に注意)。

h が単射であるには、系 2.4.71 より $\mathrm{Ker}h = \{(e, e)\}$ が必要十分であるが、

$$(g_1, g_2) \in \mathrm{Ker}h \Leftrightarrow g_1 \circ g_2 = e \Leftrightarrow g_1 = g_2^{-1} \in G_1, G_2$$

となるので、$G_1 \cap G_2 = \{e\}$ でなければこの共通部分の単位元でない元 g を用いて $(g, g^{-1}) \in \mathrm{Ker}h$ となり、単射でない。

最後の性質は、h の全射性そのものである。

逆に、これら 3 つの性質が成立したとしよう。h の群準同型性は G_1 の元と G_2 の元が可換であることから容易に従う。

単射性は上で見たように $G_1 \cap G_2 = \{e\}$ より系 2.4.71 を用いて示せる。

全射性は 3 番目の条件そのもの。 □

定義 2.6.4. $G_1, G_2 < G$ に対し、上で定義された

$$h : G_1 \times G_2 \to G, \quad (g_1, g_2) \mapsto g_1 \circ g_2$$

が群同型となっているとき、「G は部分群 G_1 と G_2 の直積である」という。

注意 2.6.5. 先に定義した「直積」は、二つの群から新しく群を構成する方法であった。ここで定義した「直積」は、ある群の構造についての言明（ステートメント）である。したがって、この両者は違うものなのであるが、同じ直積という言葉が使われている。

さて、より一般に次が成立する。証明は読者にまかせる。

命題 2.6.6. G の部分群 $G_1, \ldots, G_n$ が与えられたとする。$f(g_1, \ldots, g_n) = g_1 \circ g_2 \circ \cdots \circ g_n$ により与えられる写像（準同型とは限らないことに注意）

$$f : G_1 \times G_2 \times \cdots \times G_n \to G$$

が群準同型であるための必要十分条件は，任意の相異なる G_i, G_j に対し、G_i の任意の元と G_j の任意の元が可換であることである。

このとき、f が単射である必要十分条件は、「$g_i \in G_i$ $(i = 1, \ldots, n)$ に対し $g_1 \cdots g_n = e$ となるのは、全ての g_i が単位元であるときに限る」ことである。

第3章　群

この章では、前章で定義した群について実例を挙げて調べつつ、関連する諸概念を導入する。

3.1　対称群

3.1.1　互換・巡回置換

対称群 S_n の元を**置換** (permutation) という。 置換を具体的に記述するため、いくつかの記法を導入する。

定義 3.1.1.

互換　相異なる二元 $1 \leq i, j \leq n$ に対し、(ij) で「i と j を入れ替え、他はそのまま」という S_n の元を表し、「i と j の互換」（transposition of i and j）という。

$$(ij)(i) = j, \quad (ij)(j) = i, \quad (ij)(k) = k \quad (\text{if } k \neq i, j).$$

巡回置換 相異なる m 個の自然数 $1 \leq i_1, \ldots, i_m \leq n$ に対し、$(i_1 i_2 \cdots i_m)$ で「i_1 を i_2 に送り、i_2 を i_3 に送り、…、i_{m-1} を i_m に送り、i_m は i_1 に送る。他の元はそのまま動かさない。」という置換を表し、m 次の巡回置換 (cyclic permutation of order m) という。

互換は、$m = 2$ の場合である。なお、上のような σ を「$i_1, \ldots, i_m$」に関する巡回置換という。σ は S_n の (一つの) 巡回置換であるが、「どの元を置換するか」を明示したい場合にはこのようないいかたをする。上の σ は長さ m の巡回置換であると言われる。

$$(i_1 i_2 \cdots i_m) = (i_2 i_3 \cdots i_m i_1) = (i_3 i_4 \cdots i_m i_1 i_2) = \cdots = (i_m i_1 \cdots i_{m-2} i_{m-1})$$

であり、m 次の巡回置換の表し方はちょうど m 通りある。

一般 1 から n までの数を並べ替えたものを二組用意し、$i_1, i_2, \ldots, i_n$ および $j_1, j_2, \ldots, j_n$ とする。

$$\begin{pmatrix} i_1 & i_2 & \cdots & i_n \\ j_1 & j_2 & \cdots & j_n \end{pmatrix}$$

という記法で、i_1 を j_1 に送り、i_2 を j_2 に送り、…、i_n を j_n に送る置換を表す。

3.1.2 巡回置換への分解

集合 X 上の対称群 S_X を考える。これは、X から X への全単射の集合に、写像の合成で二項演算を定義したものであった（例 2.4.13)。いま、X を交わらない集合 T, U の直和 (§1.3.2) に分けたとする。すなわち

$$X = T \cup U, \quad T \cap U = \emptyset.$$

さて、S_X の元 f であって、T の元は T の元に、U の元は U の元に移すようなものの全体を $S_{T,U}$ で表す。

$$S_{T,U} := \{f \in S_X | f(T) = T, f(U) = U\} \subset S_X.$$

これが S_X の部分群となることは容易に示せる。S_T の元は、U 上では恒等写像にする（すなわち $u \in U \mapsto u$ と定める）ことによって $S_{T,U}$ の元と思うことができる。同様に、S_U の元を $S_{T,U}$ の元と思うことができる。これにより $S_T, S_U < S_{T,U}$ と見なすことができる。このとき、$S_T \cap S_U = \{\mathrm{id}_X\}$ となることは容易にわかる。また、S_T の元と S_U の元が可換であることは、X の任意の元の行先を追うことで確認できる。$f \in S_{T,U}$ に対して、f は $T \to T$ なる全単射を与えるから、これを f の T への制限と呼んで $f|_T \in S_T$ であらわす。同様に $f|_U \in S_U$ が定義される。$S_T, S_U < S_{T,U}$ と考えたとき、$f|_T \circ f|_U = f \in S_{T,U}$ が成立することも $x \in X$ の両辺による行先を計算することで確かめられる。上記のことを命題 2.6.3 に適用すれば

$$S_T \times S_U \cong S_{T,U}$$

が示される。

問題 3.1. 上の状況で、$f \in S_X$ ならば

$$f(T) = T \Leftrightarrow f(U) = U$$

を示せ。

特に X が有限集合のときは、

$$f(T) \subset T \Leftrightarrow f(T) = T$$

であることを示せ。無限集合の場合の反例を作れ。

問題 3.2. $X = \{1, 2, 3, \ldots, n\}$ の時 S_X を S_n と書き n 次対称群と呼んだ。ある元 $\sigma \in S_n$ が与えられたとき、σ がどのような $S_{T_1} \times S_{T_2} \times \cdots \times S_{T_k}$ に入っているかを調べるのが巡回分解 (cyclic decomposition) である。いま、$X = \coprod_{i=1}^{k} T_i$ と分割されて

$$\sigma \in S_{T_1} \times S_{T_2} \times \cdots \times S_{T_k} \tag{3.1}$$

とできたとする。目標は、このような X の分割のうちで最も細かいものを得ることである。証明したいことは、そのような分割をとった時、$\sigma|_{T_i}$ は T_i に関する巡回置換であることである。

以下、σ と T_i は (3.1) を満たすとし、T_i はそのような分割の中で最も細かいものと仮定する。

1. X の元 t_1 を任意にとる。$t_1 \in T_1$ と仮定して一般性を失わない。$\sigma^m(t_1) \in T_1$ $(m \in \mathbb{N})$ を示せ。また、$\sigma|_{T_1}$ が T_1 に関する巡回置換であることを示せ。(T_1 が一元集合である可能性もある。この時は、$\sigma|_{T_1}$ は恒等置換であるが、「長さ 1 の巡回置換」とみなすことにする。)

2. 上であらわれた $\{\sigma^m(t_1)|m=0,1,2,\ldots\}$ を t_1 の σ-軌道 (orbit) という。上のように T_1 を t_1 の σ-軌道としたとき、$\sigma \in S_{T_1} \times S_{T_1^c}$ を示せ。ここに T_1^c は、T_1 の X における補集合である。

3. $T_1^c = \emptyset$ ならば $T_1 = X$ で、(3.1) を満たす分解は $X = T_1$ しかなく、σ は T_1 に関する巡回置換となり、題意の証明は終わる。そうでないとして、T_1^c から任意に t_2 をとる。t_2 の σ-軌道を T_2 とする。すると、

$$\sigma \in S_{T_1} \times S_{T_2} \times S_{(T_1 \cup T_2)^c}$$

であることを示せ。

4. この要領で、次々に σ-軌道をとっていくことにより、

$$\sigma \in S_{T_1} \times \cdots \times S_{T_k},$$

T_i はどれも σ-軌道、というように分解される。これが所望の分解、すなわち (3.1) を満たす最も細かい分割であり、直積分解 $\sigma = \sigma|_{T_1}\sigma|_{T_2}\cdots\sigma|_{T_k}$ において、$\sigma|_{T_i}$ は T_i に関する巡回置換であることを示せ。

上の分解を行うと，

$$\sigma = \sigma_1 \circ \sigma_2 \circ \cdots \circ \sigma_k$$

と分解され，σ_i 同士は可換で、各 σ_i は T_i に関する巡回置換になっている。このような分解は、σ_i の順番の入れ替えを除いてただ一通りである。これを σ の**巡回置換への分解**、または**巡回分解**という。

問題 3.3. 上で，σ の位数は、σ_i の位数の最小公倍数、すなわち $\#(T_i)$ の最小公倍数であることを示せ。

例 3.1.2.

$$\sigma := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix} \in S_5$$

を巡回分解する。1 の軌道を見ると

$$1 \mapsto 3 \mapsto 5 \mapsto 1$$

となっているから、$T = \{1,3,5\}$ が 1 の軌道であり

$$\sigma|_T = (135)$$

である。この軌道の外にある 2 をとり、その軌道をみると

$$2 \mapsto 4 \mapsto 2$$

となるから $U = \{2,4\}$ ととれば

$$\sigma|_U = (24)$$

である。この二つの軌道で $\{1,2,3,4,5\}$ を尽くしているので、

$$\sigma = (135)(24) = (24)(145).$$

この元の位数は、問題 3.3 により $\mathrm{LCM}(3,2) = 6$ である。

巡回分解のしかたは、あらわれる各巡回置換の順番の入れ替え（上の例で言うと $(135)(24) = (24)(145)$ なる二通り）を除いて一意的である。これは、「軌道に分解する」という巡回分解の計算の仕方から明らかであろう。

S_n の元の位数を求めよう。1 の行き先の選び方は n 通りある。それを決めた上で、2 の行き先を考えると 1 の行き先と衝突しないようにしないとならないので $n-1$ 通りある。つまり、1 と 2 のかさならないような行き先は $n(n-1)$ 通りある。次に 3 の行き先を考えると、先の $1,2$ の行き先二つと衝突しないように選ばないとならないので $n-2$ 通りある。こうして、$\{1,2,3\}$ から $\{1,2,\dots,n\}$ への単射の個数は $n(n-1)(n-2)$ となる。より一般に、m 元集合 $\{1,2,\dots,m\}$ から n 元集合 $\{1,2,\dots,n\}$ への単射の数は

$$ {}_nP_m = n(n-1)(n-2)\cdots(n-m+1) $$

通りある。S_n の元の数は $m=n$ のときなので

$$ \#(S_n) = n(n-1)\cdots 2\cdot 1 = n! $$

である。

3.2 共役類

群 G の元 a,b が互いに共役であるとは、ある $g\in G$ が存在して

$$ a = gbg^{-1} $$

が成り立つことである。この二項関係は G 上の同値関係であることが容易に確かめられ、**共役関係** (conjugacy relation) と呼ばれる。ここでは

$$ a \sim_{\mathrm{conj}} b $$

で表す。この同値関係による同値類を、**共役類**と呼ぶ。

問題 3.4. 共役な元の位数は互いに等しいことを示せ。

定義 3.2.1. $\sigma\in S_n$ に対し、σ を巡回分解して

$$ \sigma = (\text{長さ } r_1 \text{ の巡回置換})(\text{長さ } r_2 \text{ の巡回置換})\cdots(\text{長さ } r_k \text{ の巡回置換}) $$

としたとする。ここで、順番を入れ替えて

$$ r_1 \geq r_2 \geq \cdots \geq r_k \geq 1 $$

とする。ここで、σ が動かさない元 $\ell\in\{1,2,\dots,n\}$ に対しては、軌道は一個であり長さ 1 の巡回置換 (ℓ) は単位元となる。従ってこのような長さ 1 の巡回置換を巡回分解にいれなくても良さそうではあるが、意図的にこれらもすべて書き下して、1 から n の全ての元が（ちょうど一度ずつ）上の分解に現れるように記述することにする。すなわち

$$ r_1 + r_2 + \cdots + r_k = n $$

となる。このとき、数の列 $(r_1,r_2,\dots,r_k)$ を σ の**巡回分解型**という。

命題 3.2.2. S_n の二つの元が共役である必要十分条件は、巡回分解型が同じであることである。

証明. (十分性) $a, b \in S_n$ の巡回分解が同じとすると、

$$a = (i_1 i_2 \cdots i_{r_1}) \cdots (j_1 j_2 \cdots j_{r_k}), \quad b = (s_1 s_2 \cdots s_{r_1}) \cdots (t_1 t_2 \cdots t_{r_k}),$$

となる。ここで、$g \in S_n$ を

$$g : i_1 \mapsto s_1, i_2 \mapsto s_2, i_3 \mapsto s_3, \ldots, i_{r_1} \mapsto s_{r_1}, \ldots, j_1 \mapsto t_1, j_2 \mapsto t_2, \ldots, j_{r_k} \mapsto t_{r_k}$$

で定義すると、

$$g^{-1} b g = a$$

となることがわかり、証明が終わる。どうしてそうなるかというと、例えば i_3 の $g^{-1}bg$ による行き先をおっかけると

$$i_3 \overset{g}{\mapsto} s_3 \overset{b}{\mapsto} s_4 \overset{g^{-1}}{\mapsto} i_4$$

となり、

$$i_3 \overset{a}{\mapsto} i_4$$

と一致している。どの元でも同様に、$g^{-1}bg$ による送り方と a による送り方が一致することがわかり、証明が完成する。

(必要性) $a = g^{-1}bg \in S_n$ と仮定して、b の巡回分解型と a の巡回分解型が一致することを示す。問題 3.2 においてみたように、b の巡回分解型は、$X = \coprod_{i=1}^{k} T_i$ という分割から $\#(T_i)$ の列として決まる。これら T_i はそれぞれ b の軌道として決まる。ここで、$X = \coprod_{i=1}^{k} g^{-1}(T_i)$ という分割をあらたに考える。(S_n が群であるので、g^{-1} を施す写像は可逆であり、あらたな分割を与える。) $t_i \in T_i$ は b により $b(t_i) \in T_i$ に移され、T_i は b の t_i を含む軌道となる。全てに g^{-1} を施す（これは可逆射である）と、$g^{-1}(t_i) \in g^{-1}(T_i)$ は $a = g^{-1}bg$ により $a(g^{-1}(t_i)) = g^{-1}bgg^{-1}(t_i) = g^{-1}(b(t_i)) \in g^{-1}T_i$ にうつされる。T_i が b に関する軌道であることから、$g^{-1}(T_i)$ が a に関する軌道であることが従う。g^{-1} を掛ける写像は可逆であるから $\#(T_i) = \#(g^{-1}(T_i))$ である。$\#(g^{-1}(T_i))$ がなす数列が a の巡回分解型であるから、これは b のそれに一致する。 □

3.3　中国式剰余定理

m, n を自然数とする。$q_m : \mathbb{Z} \to \mathbb{Z}/m$ を加法群から加法群への商準同型とする。$\mathrm{Ker} q_m = m\mathbb{Z}$ であり、$mn\mathbb{Z} \subset m\mathbb{Z}$ であるから定理 2.4.77 より

$$\bar{q_m} : \mathbb{Z}/(mn) \to \mathbb{Z}/m$$

なる群準同型が与えられる。この写像は

$$[a]_{mn} \mapsto [a]_m$$

で与えられる。平たく言えば、mn で割った余りを、さらに m で割った余りに落とすという写像である。

同様に、

$$\bar{q_n} : \mathbb{Z}/(mn) \to \mathbb{Z}/n$$

が与えられる。

定理 3.3.1. (**中国式剰余定理**)

$$(\bar{q_m}, \bar{q_n}) : \mathbb{Z}/(mn) \to \mathbb{Z}/m \times \mathbb{Z}/n, \quad [a]_{mn} \mapsto ([a]_m, [a]_n)$$

が全単射である必要十分条件は、m と n が互いに素であることである。

証明. 十分性：この写像の核の元 $[a]_{mn}$ を考えると $[a]_m = 0$, $[a]_n = 0$ となる。これは、a が m でも n でも割り切れることを意味する。これは a が m, n の公倍数ということであるが、互いに素であるから mn の倍数となり、従って $[a]_{mn} = 0$。系 2.4.71 より、単射性が言えた。

両辺は元の数が mn の有限集合であるから、単射性から全射性が従う (命題 1.1.28)。

必要性：m, n が互いに素でないとすると、m, n の最小公倍数 a は mn 未満であり、従って $[a]_{mn} \neq 0$ である。だが公倍数であるから $[a]_m = 0$, $[a]_n = 0$ であり、従って核に入る単位元でない元。従って単射にならない。 □

注意 3.3.2. $(\bar{q_m}, \bar{q_n})$ は和も積も保つ。従って、m, n が互いに素なときには加法群としての同型であり、積に関するモノイドとしての同型である。

（後述するように環同型である。）

これを用いると、オイラー関数 $\varphi(n)$ を効率的に計算することができる。

補題 3.3.3. G_1, G_2 をモノイドとすると、

$$(G_1 \times G_2)^\times = G_1^\times \times G_2^\times.$$

問題 3.5. 上の補題を証明せよ。

系 3.3.4. m, n を互いに素な自然数とするとき、

$$(\mathbb{Z}/(mn))^\times \cong \mathbb{Z}/m^\times \times \mathbb{Z}/n^\times.$$

両辺の元の個数を比べて

$$\varphi(mn) = \varphi(m)\varphi(n).$$

証明. 定理 3.3.1 の全単射は積に関するモノイドの同型であった。これに上の補題を適用すれば上の式を得る。 □

補題 3.3.5. $(\mathbb{Z}/(p^n))^\times$ は $p^n - p^{n-1}$ 個の元からなる。すなわち $\varphi(p^n) = p^n - p^{n-1}$。

証明. 0 以上 p^n 未満の数 (p^n 個ある) のうち、p と互いに素なもの（つまり p の倍数とならないもの）を数えれば $\varphi(p^n)$ が求まる。この補集合である「p の倍数」は、$0, p, 2p, \ldots, p^{n-1}p$ であり p^{n-1} 個ある。よって $\varphi(p^n) = p^n - p^{n-1}$. □

命題 3.3.6. $n = p_1^{e_1} \cdots p_s^{e_s}$ と素因数分解したとき、$\varphi(n) = (p_1^{e_1} - p_1^{e_1 - 1}) \cdots (p_s^{e_s} - p_s^{e_s - 1})$。

証明. $\varphi(n) = \varphi(p_1^{e_1}) \cdots \varphi(p_s^{e_s})$ より従う。 □

3.4　作用

3.4.1　群の集合への作用

集合 S の集合 X への作用とは

$$f : S \times X \to X$$

の形の写像のことであった。定理 1.1.30 によれば、これを与えることと

$$\rho : S \to \mathrm{Map}(X, X)$$

を与えることとは同値である。$s \in S$ に対し $\rho(s) : X \to X$ であるから $\rho(s)(x) \in X$。これを

$$s \cdot x := \rho(s)(x)$$

と表記することが多い。

例 3.4.1. X を集合、S_X を X 上の対称群とする。

$$S_X \times X \to X, \quad (\sigma, x) \mapsto \sigma(x)$$

により、S_X は X に作用する。

例 3.4.2. K を体とする。行列環 $M_n(K)$ と n 次元縦ベクトルの掛け算は、

$$M_n(K) \times K^n \to K^n, \quad (A, \mathbf{x}) \mapsto A\mathbf{x}$$

なる作用を与える。

定義 3.4.3. 集合 S, X と S の X への作用

$$\rho : S \to \mathrm{Map}(X, X)$$

が与えられているとする。

1. S がマグマ $(S, \circ_S)$ であるとき、ρ が「マグマとしての S の X への作用」であるとは ρ が

   $$(S, \circ_S) \to (\mathrm{Map}(X, X), \circ)$$

   なるマグマ準同型であることである。さらに S が半群であるとき「S の X への半群作用」という。

2. S がモノイド $(S, \circ_S, e_S)$ とする。ρ が

   $$(S, \circ_S, e_S) \to (\mathrm{Map}(X, X), \circ, \mathrm{id}_X)$$

   なるモノイド準同型であるとき、「S の X へのモノイド作用」という。

3. S が群 $(S, \circ_S, e_S)$ とする。ρ が

   $$(S, \circ_S, e_S) \to (\mathrm{Map}(X, X)^\times, \circ, \mathrm{id}_X)$$

   なる群準同型であるとき、「S の X への群作用」という。

問題 3.6. 定義 3.4.3 と同じ設定とする。以下を確かめよ。

1. S がマグマ（あるいは半群）であるとき、ρ がマグマとしての作用（あるいは半群作用）である必要十分条件は

   AB $\forall s_1, s_2 \in S, \forall x \in X, \rho(s_1)(\rho(s_2)(x)) = \rho(s_1 \circ_S s_2)(x)$

   をみたすことである。言い換えると、

   $$s_1 \cdot (s_2 \cdot x) = (s_1 \circ_S s_2) \cdot x$$

   となることである。

2. S がモノイドであるとき、ρ がモノイド作用となる必要十分条件は、上の **AB** に加えて

   AC $\rho(e_S) = \mathrm{id}_X$

   を満たすことである。言い換えると

   $$\forall x \in X, e_S \cdot x = x$$

   を満たすことである。

3. S が群であるとき、ρ が群作用であるとは上の **AB**、**AC** に加えて

   AD $\rho(s^{-1}) = \rho(s)^{-1}$

   が成立することである。

   しかし、命題 2.4.20 により、S が群であるときには **AB** と **AC** から **AD** は従うことがわかる。

定義 3.4.4. G をモノイドとする。G の X への作用が上の **AB**, **AC** を満たすとき、この作用を**モノイド G の X への作用** (action of the monoid G on X) という。

定義 3.4.5. G を群とする。G の X への作用が上の **AB**, **AC** を満たすとき (したがって **AD** も満たす)、この作用を**群 G の X への作用** (action of the group G on X) という。

注意 3.4.6. 多くの文献で、やや用語が混乱している。G が群であれば「G の X への作用」と言ったら「群 G の X への作用」のことを指す、という約束になっている本が多い。この本では、前者は単なる写像 $G \times X \to X$ を指し、後者は条件 **AB**, **AC** を満たす作用のことを指すこととする。

定義 3.4.7. $(G, \circ)$ を群とし、$X = G$ とする。$G \times X \to X$ を $(g, x) \mapsto g \circ x$ で定義すると、群 G の集合 G への作用となる。これを G の G への**左正則作用**という。

実は、いままで扱ってきた「マグマ作用」「群作用」は、本来**左作用**と呼ばれるものである。次の定義を見れば、なぜ左作用と呼ぶべきか理解できると思う。

定義 3.4.8. X を集合、$(S, \circ)$ をマグマとする。写像 $\cdot : X \times S \to X$ が

AB' $\forall s_1, s_2 \in S, \forall x \in X, (x \cdot s_1) \cdot s_2 = x \cdot (s_1 \circ s_2)$

を満たすとき、マグマ S の X への**右作用**という。

区別がつきにくいので、もう少し解説する。写像 $\cdot : X \times S \to X$ も「S の X への作用」である。$s \in S$ を一つ決めたとき、$x \mapsto x \cdot s$ は写像 $\mathrm{Map}(X, X)$ の元を与えるから、これを $\rho'(s) : x \mapsto x \cdot s$ で表すことにする。すると、右作用の定義は

$$\rho'(s_2)(\rho'(s_1)(x)) = \rho'(s_2)(x \cdot s_1) = (x \cdot s_1) \cdot s_2 = x \cdot (s_1 \circ s_2) = \rho'(s_1 \circ s_2)(x)$$

と表される。言い換えれば $\rho' : (S, \circ) \to (\mathrm{Map}(X, X), \circ)$ が

$$\rho'(s_1 \circ s_2) = \rho'(s_2) \circ \rho'(s_1) \tag{3.2}$$

を満たすとき、ρ' はマグマ S の右作用を与えることになる。ここで、逆マグマの定義をしよう。

定義 3.4.9. マグマ $(M, \circ)$ に対し、その逆マグマ $(M, \circ)^{\mathrm{op}} = (M, \circ')$ を次のように定義する (これもマグマである)。台集合は元のマグマと同じ M であるが、二項演算は

$$s_1 \circ' s_2 := s_2 \circ s_1$$

により定義する。

同様にして、半群、モノイドまたは群である G に対して、二項演算の順序を反転することにより逆半群、逆モノイド、逆群 G^{op} が定義される。(単位元、逆元をとる演算は、もとのモノイドや群と同一である。) 「逆半群」は半群であり、「逆モノイド」はモノイドであり、「逆群」は群である。

この用語を用いれば、例えば群 G の集合 X への右作用とは、モノイド準同型

$$G \to (\mathrm{Map}(X, X), \circ)^{\mathrm{op}}$$

に他ならない。こうして、右作用に関する理論は左作用に関する理論とほぼ平行に進められる。特にこの本では、右作用は取り扱わず、群作用 (あるいはマグマ作用、半群作用、モノイド作用) と言ったら左作用のみを扱うことにする。

3.4.2 作用の軌道

定義 3.4.10. $\cdot : S \times X \to X$ を集合 S の X への作用とする。$x \in X$ に対し、x の S **軌道** (S-orbit) を

$$S \cdot x := \{s \cdot x | s \in S\}$$

で定義する。

節 2.4.8 で「群の概念と同値関係の概念は親戚である」ことをみたが、次の命題もこれらの概念の近さを示している。

命題 3.4.11. $(G, \circ)$ を群とし、$\cdot : G \times X \to X$ を G の群としての X への作用とする。このとき、二項関係 $x \sim_G x'$ を $x \in G \cdot x'$ で定義すると、同値関係になる。x の属する同値類は軌道 $G \cdot x$ である。

証明. 定義 1.3.7 [E1], [E2], [E3] を確かめればよいが、どれも難しくない。 □

定義 3.4.12. $\sim_G$ に関して X を同値類に分割したものを、X の G による**軌道分解**といい、この商集合を $G\backslash X$ で表わす。軌道が唯一つになるとき、作用が**推移的 (transitive)** であるという。

問題 3.7. G を群とする。G の G への左正則作用は推移的であることを示せ。

定義 3.4.13. $\cdot : G \times X \to X$ を群の集合への作用とする。$x \in X$ に対し、G の x における**安定化部分群** (stabilizer of x, stabilizing subgroup of x) を

$$G_x := \{g \in G | g \cdot x = x\}$$

で定義する。

問題 3.8. G_x が G の部分群であることを示せ。

命題 3.4.14.

$$f : G \to G \cdot x, \quad g \mapsto g \cdot x$$

なる写像は

$$\bar{f} : G/G_x \to G \cdot x$$

なる全単射を引き起こす。

証明. f は定義から全射である。集合の準同型定理 1.3.33 より

$$f(g) = f(g') \Leftrightarrow g'^{-1} \circ g \in G_x$$

を言えばよいが、$f(g) = gx = g'x = f(g')$ で g' を移項すると $g'^{-1}g \in G_x$。これより従う。 □

例 3.4.15. K を体とし、$G = GL_n(K)$ を n 次正則行列の集合、$M = M_n(K)$ を n 次正方行列の集合とする。行列の積

$$\mu : G \times M \to M$$

は G の群作用である。また、共役作用と呼ばれる

$$c : G \times M \to M, \quad (P, A) \mapsto PAP^{-1}$$

も G の群作用である。以下、作用は c を考える。$A \in M$ の軌道は A と共役な行列、すなわち $P^{-1}AP$ の形の行列の全体である。

Jordan 標準形と呼ばれる理論をもちいると、$K = \mathbb{C}$ のときは、$P^{-1}AP$ を Jordan 標準形という形にできることがわかる。これは、各軌道から一つ代表元を探して持ってくる、という方法の一つである。

すなわち、この作用による軌道分解 $G\backslash M$ と、Jordan 標準形（のブロックの入れ替えを同一視したもの）とが 1 対 1 に対応している。

A の軌道について。$A \in M$ の安定化部分群 G_A は、A と可換な正則行列の全体である。従って、集合としての全単射

$$\{PAP^{-1} | P \in G\} \cong G/G_A$$

がある。

3.4.3　対称群の元の巡回分解に関する再考

$X = \{1, 2, \ldots, n\}$ とする。n 次対称群 $S_n = S_X$ は X に自然に群として作用していた：$\sigma \in S_n, x \in X$ に対して $\sigma(x) \in X$ が定まり、群同型 $S_n \to \mathrm{Map}(X, X)^\times$ を与えていた。今、$\sigma \in S_n$ を一つ固定し、群 $G < S_n$ を $G :=< \sigma >$ で定義すれば、群準同型 $G \to \mathrm{Map}(X, X)^\times$ が与えられる。したがって命題 3.4.11 とそれに続く定義により、X は G 軌道に分割される。これが問題 3.2 にあらわれた X の分割であり、各軌道 T_i に制限すると σ は T_i に関する巡回置換となっている。このように、「置換の巡回分解」は、軌道分解の一例と考えることができる。

3.4.4　代数構造をもつ集合への作用

X に代数構造が入っていると、**自己準同型 (endomorphism) モノイド** $\mathrm{End}(X)$ が定義できる。「代数構造とは何か」については 2.4.6 節で多少説明したが、読者はそういった一般論より、代数構造の具体例（加法群など）について理解することに努めた方が良いと思われる。例えば X が加法群であれば $\mathrm{End}(X)$ は X から X への群準同型の集合である。X が体 K 上の線形空間であれば $\mathrm{End}(X)$ は X から X 自身への体 K 上の線形写像の全体である。（元来は、「どの代数構造に着目しているか」を明示するために、前者については $\mathrm{End}_{\text{加法群}}(X)$ と書くべきであり、後者は $\mathrm{End}_{K\text{ 線形空間}}(X)$ と書くべきであるが、この本では省略して $\mathrm{End}(X)$ と書いてしまっている。なお、「体」に不慣れな人は、以下で K を実数の集合と考えてもこの節の理解になんら不都合はない。）$\mathrm{End}(X)$ は合成 $\circ$ と単位元 id_X によりモノイドとなる。$\mathrm{End}(X)$ の可逆元の集合 $\mathrm{End}(X)^\times$ は命題 2.4.9 により群となる。この群を $\mathrm{Aut}(X)$ と書き、X の**自己同型群 (automorphism group)** という。

定義 3.4.16. S を集合、X を代数構造を指定された集合とする（この言い方が抽象的過ぎると感じる読者は、X を加法群と思ってよい）。写像

$$\rho : S \to \mathrm{End}(X) \tag{3.3}$$

を、代数構造をもつ集合 X への S の作用という。

実は、上のような場合、S にも代数構造が入っていることがほとんどである。これについては次節で説明する。

例 3.4.17. K を体とする。X を n 次元縦ベクトル空間 K^n とするとき、$\mathrm{End}(X)$ は K^n からそれ自身への K 線形写像全体の集合をあらわす。n 次正方行列の集合を $M_n(K)$ であらわす。$A \in M_n(K)$ に対し、A を X の元に左から掛ける写像 L_A を

$$L_A : X \to X, \quad \mathbf{x} \mapsto A\mathbf{x}$$

で定義すると、

$$\rho : M_n(K) \to \mathrm{End}(X), A \mapsto L_A$$

なる $M_n(K)$ の線形空間 X への作用が定まる。

$M_n(K)$ は単なる集合ではなく、「環」という代数構造を持つ。特に、積についてモノイドであり、和について加法群となっている。上記の ρ は $M_n(K)$ を積でモノイドと見たとき、モノイド準同型となっている。

$$L_{AB}(\mathbf{x}) = (AB)\mathbf{x} = A(B\mathbf{x}) = L_A(L_B(\mathbf{x})) = (L_A \circ L_B)\mathbf{x}$$

より従う。(単位元についてもチェックが必要だがここでは省略する。) 一方、$M_n(K)$ を加法群としてみたときには、ρ は一般にモノイド準同型とならない。実際、

$$L_{(A+B)}(\mathbf{x}) = (A+B)\mathbf{x} = A\mathbf{x} + B\mathbf{x} = (L_A + L_B)(\mathbf{x}) \tag{3.4}$$

が成立するが、ρ が $(M_n(K), +)$ から $(\mathrm{End}(X), \circ)$ へのモノイド準同型となるためには右辺は $(L_A \circ L_B)(\mathbf{x})$ となるべきであるからである。これが注意 3.4.6 で述べたことの一つの例である。「$M_n(K)$ の $X = K^n$ への自然な作用」と言ったら数学者はみな暗黙の了解で ρ を思い浮かべるが、「ρ が加法群 $(M_n(K), +)$ の $X = K^n$ への作用になっていない」ということは「当たり前すぎて気づいていない」いないのである。なぜなら、そんなことを心配するよりも「環の加群への作用」という概念を勉強するほうが大切だからである。先走って説明する。X が加法群であるので、$\mathrm{End}(X)$ も自然に加法群である。$f, g \in \mathrm{End}(X)$ に対して $(f+g)(x) := f(x) + g(x)$ で和が定義できる。すると、ρ は $(M_n(K), +) \to (\mathrm{End}(X), +)$ なる加法群準同型を与えている。(3.4) がその証明を与えている。より詳しく言えば $\rho : (M_n(K), \text{積}, +) \to (\mathrm{End}(X), \circ, +)$ は環準同型となっている。このような扱いは、「環と加群」の章 5.1 で述べる。

3.4.5 群の、代数構造を持つ集合への作用

作用 $S \times X \to X$ について、節 3.4.1 では S に代数構造が入っており X には入っていない場合を扱った。逆に、節 3.4.4 では、S がただの集合で、X に代数構造が入っている場合を扱った。ここでは、S にも X にも代数構造が入っている場合を扱う。

定義 3.4.18. X を加法群とし、S をマグマ (半群、モノイド) とする。マグマ (半群、モノイド) 準同型

$$\rho : S \to \mathrm{End}(X)$$

を S の加法群 X へのマグマ (半群、モノイド) 作用という。S が群であるときは、モノイド準同型

$$\rho : S \to \mathrm{End}(X)$$

を S の加法群 X への群作用 (group action) という。このとき、X を S-加群 (S-module) という。ρ を S の X における表現という。

ρ の像は $\mathrm{Aut}(X)$ に入る（例えば命題 2.4.20 を $f = \rho$ に対して使えばよい）ので、群準同型

$$\rho : S \to \mathrm{Aut}(X)$$

を S の X への群作用という、といっても良い。

上の定義で、X は加法群としたが、線形空間としても同様の定義がなされる。あるいはモノイド、群としてもよい。（一般の代数構造としても、同様の定義ができるがその考察はここではしない。）

例 3.4.19. (定義 3.4.7 参照。) $(S, \cdot)$ をマグマとする。$a, b \in S$ に対して $L_a(b) := a \cdot b$ とおくと $L_a \in \mathrm{Map}(S, S)$。こうして与えられる

$$\rho : S \to \mathrm{Map}(S, S), \quad a \mapsto L_a$$

を S の左正則作用 (left regular action) という。

ρ が $(S,\cdot) \to (\mathrm{Map}(S,S),\circ)$ なるマグマ準同型であるという条件を記述すると

$$L_{a\cdot b} = L_a \circ L_b$$

すなわち

$$L_{a\cdot b}(c) = L_a \circ L_b(c)$$

であるが、これは

$$(a\cdot b)\cdot c = a\cdot(b\cdot c)$$

と書き直せる。すなわち、$(S,\cdot)$ が半群であることと S の左正則作用がマグマ作用であることとは同値である。

例 3.4.20. $(M,+,0)$ を加法群とする。$f,g \in \mathrm{End}(M)$ に対して $f +_{\mathrm{End}(M)} g \in \mathrm{End}(M)$ を

$$(f +_{\mathrm{End}(M)} g)(x) := f(x) +_M g(x)$$

で定義すると、加法群になる。

一方、合成 $\circ$ により $(\mathrm{End}(M),\circ,\mathrm{id}_M)$ はモノイドである。

$$f\circ(g+h) = f\circ g + f\circ h, \quad (f+g)\circ h = f\circ h + g\circ h$$

が証明できるので、$\mathrm{End}(M)$ は環となる。

M が K 線形空間であるときも同様のことが言える。特に $\mathrm{End}(K^n)$ は環である。$\mathrm{End}(K^n)$ と $M_n(K)$ の間には自然な一対一対応があり、これが行列の集合が環となる理由である。

例 3.4.21. $(M,+,0)$ を加法群とし、$(M,\cdot)$ を同じ集合に入ったマグマの構造とする。$L_a(b) = a\cdot b$ とし、

$$\rho : M \to \mathrm{Map}(M,M), \quad a \mapsto L_a$$

を考える。この ρ が

$$\rho : M \to \mathrm{End}(M) \ \ (\subset \mathrm{Map}(M,M))$$

なる加法群の準同型である条件を書き下してみると二つの条件：

1. ρ の像が $\mathrm{End}(M)$ に入る
2. ρ が準同型である

に分けられる。

前者は $\rho(a) : M \to M$ が単なる写像ではなく準同型であるということであるから

$$\rho(a)(b+c) = \rho(a)(b) + \rho(a)(c)$$

ということであり、言い換えると

$$a\cdot(b+c) = a\cdot b + a\cdot c$$

であることである。

後者の条件は

$$\rho(a+b)(c) = (\rho(a) + \rho(b))(c)$$

すなわち

$$(a+b)\cdot c = a\cdot c + b\cdot c$$

である。環の定義における分配法則はこのようにして自然に現れる。

第4章　環

4.1　環の定義

環と体の定義は定義 2.5.1 で与えた。が、ここで復習しておく。

定義 4.1.1. 環 (英語 ring) R とは、集合 R とその上の二つの二項演算 $+, \cdot$ の組 $(R, +, \cdot)$ であって、次の三つの公理（環の公理という。）を満たすもの。

R1 $(R, +)$ は加法群をなす。この単位元を $0 \in R$ であらわす。

R2 $(R, \cdot)$ は半群をなす。

R3 (分配法則) 任意の $a, b, c \in R$ に対して $(a+b)\cdot c = (a\cdot c)+(b\cdot c)$, $a\cdot(b+c) = (a\cdot b)+(a\cdot c)$ が成立する。

さらに、次の条件

R2' (積の単位元と呼ばれる)$1 \in R$ が存在し、$(R, \cdot, 1)$ が 1 を単位元とするモノイドとなる

を満たすとき、$(R, +, 0, \cdot, 1)$ を単位的環（英 ring with unit）という。
環 $(R, +, 0, \cdot)$ に対して条件

R4 (積の可換性）$(R, \cdot)$ が可換な半群である、すなわち任意の $a, b \in R$ に対して $a \cdot b = b \cdot a$

が成り立つとき、R を可換環 (commutative ring) という。可換環でない環を非可換環という。
単位的環で可換なものを単位的可換環という。
単位的可換環であって、 0 以外の元が積に関して群をなすもの、すなわち条件

F モノイド $(R, \cdot, 1)$ において、$1 \neq 0$ でかつ 0 以外の元は全て可逆元

を満たすとき、R は可換体 (commutative field)、または体 (field) であるという。

ややこしいが、要するに和と積が定義されて、和に対して可換群、積に対して半群で、分配法則が満たされるものを環という。積に関する単位元が存在するとき、単位的環という。積に関して可換なとき、可換環という。

注意 4.1.2. 定義 2.5.1 で定義した環は、こちらでいう単位的環である。現在、単に「環」といったら単位的可換環を指すことが多いが、数学の分野によって慣習が違う。初学者には混乱するところである。
特に、「単位的」という言葉は省略されることが多い。

4.2 環の例と環準同型

例 4.2.1. 1. 整数の集合 $\mathbb{Z}$ は和と積に関して可換環となる。積の単位元 1 も存在し、単位的可換環である。

2. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ は可換体である。

3. $\mathbb{Z}/n$ は (単位的) 可換環である。これが体になる必要十分条件は、n が素数であることである (命題 2.5.3)。

4. R を環とするとき、行列環 $M_n(R)$ は環である。R が単位環なら $M_n(R)$ もそうである。R が可換であっても、$n \geq 2$ なら $M_n(R)$ は非可換な環となる。

5. R を可換環とすると、R 係数の一変数多項式の集合 $R[t]$ は可換環である (§4.3)。R が単位的ならば $R[t]$ もそうである。

問題 4.1. R を環とする。和の単位元 0 に対して、

$$\forall a \in R, 0 \cdot a = a \cdot 0 = 0$$

が成立することを示せ。

ヒント:和の単位元の定義より $0 = 0 + 0$。分配法則より $0 \cdot a = (0 + 0) \cdot a = 0 \cdot a + 0 \cdot a$。両辺に $-(0 \cdot a)$ を足して示せる。

問題 4.2. R が単位的可換環のとき、$(-1) \cdot a = -a$ を示せ。

定義 4.2.2. 単位的環 R で $0 = 1$ が成立するとすると、$R = \{0\}$ となる。このような環を零環という。

$1 = 0$ ならば問題 4.1 から

$$x = 1x = 0x = 0$$

より全ての元は 0 である。零環は定義より体ではない。また、整域（後述）でもない。

問題 4.3. 単位的環 R において、0 が積について可逆ならば R は零環であることを示せ。こうして、体の定義における「0 以外の元が可逆」という条件で 0 が特別扱いされなくてはならない理由がわかる。

代数構造における準同型とは、「与えられた全ての演算を保つ写像」のことであった。(単位的) 環 R においては、与えられている演算は加法 $+$、加法の単位元 0、加法に関する逆元 $-$、積、積の単位元 1 の 5 つが与えられている。

定義 4.2.3. R_1, R_2 を（単位的）環とする。R_1 から R_2 への（単位的）環準同型とは写像 $f : R_1 \to R_2$ であって

$$f(x +_1 y) = f(x) +_2 f(y), \quad f(x \cdot_1 y) = f(x) \cdot_2 f(y), \text{さらに単位的環の場合は} \quad f(1_1) = 1_2$$

の二つ（単位的環の場合は三つ）を満たすもののことである。

0 と − はどこへいっちゃったのかといえば、命題 2.4.19 があるから最初の一つを満たすと自動的に $0, -$ を f は保つ。

定義 4.2.4. R_1, R_2 を (単位的) 環とする。$f : R_1 \to R_2$, $g : R_2 \to R_1$ を互いに逆射である環準同型としたとき、f を環同型という。そのような f が存在するとき、R_1 と R_2 は環同型であるという。

命題 4.2.5. $f : R_1 \to R_2$ が環準同型かつ全単射であることと、環同型であることとは同値である。

問題 4.4. 上の命題を証明せよ。難しいのは「環準同型 f が逆写像 g を持つなら、g も環準同型になること」だが、命題 2.1.13 を和と積についてそれぞれ使えばよい。

問題 4.5. 商写像

$$q : \mathbb{Z} \to \mathbb{Z}/n$$

は (単位) 環準同型であることを示せ。

命題 4.2.6. R を単位的環とする。整数環 $\mathbb{Z}$ から R への単位環準同型が唯一つ存在する。

証明. 存在すると仮定する。単位環準同型なので $1_{\mathbb{Z}}$ を 1_R に移す。加法群としての準同型でこのようなものは系 2.4.52 により唯一つ存在するので、あるとしたらこれに一致する。すなわち存在すれば唯一つ。この系において、乗法的に書くときには $n \mapsto g^n$ と書くが、行き先が加法群のときには ng とかく。

$n \in \mathbb{Z}$ に対して $n1_R$ を対応させる写像が環準同型であることを示せばよい。加法群としての準同型であることは系 2.4.52 で示されているから、あとは積を保つこと

$$(nm)1_R = (n1_R) \cdot (m1_R)$$

と単位元を保つこと

$$1(1_R) = 1_R$$

を言えばよいが、これは $n1_R$ の定義から分配法則を繰り返して得られる。 □

定義 4.2.7. R を (単位) 環とする。R の部分集合 S が R の部分 (単位) 環であるとは、(単位) 環として指定された全ての演算について閉じていることである。具体的に言えば

- $a, b \in S \Rightarrow a + b \in S$
- $0 \in S$
- $a \in S \Rightarrow -a \in S$

が成り立つ、すなわち加法について S は R の部分群 (定義 2.4.23) であり、

- $a, b \in S \Rightarrow a \cdot b \in S$
- 単位的環であるときには $1 \in S$

が成り立つ、すなわち積について S は R の部分半群（命題 2.2.9) であることである。単位的環であるときは S は R の部分モノイド (定義 2.3.17）であることである。

このとき、S は環（単位的環）となる。

例 4.2.8. 1. $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ は全て単位的可換環としての部分環である。

2. 偶数の集合 $2\mathbb{Z}$(この記法については定義 2.4.40) は $\mathbb{Z}$ の部分環であるが、単位的環としての部分環ではない。

3. m, n を互いに素な自然数とする。

$$am + bn = 1$$

となる整数 a, b を取る (定理 2.4.64)。$f : \mathbb{Z}/m \to \mathbb{Z}/mn$ を $[x]_m \mapsto [bnx]_{mn}$ で定義する。これは well-defined であり、環準同型となっている。加法群としての準同型であることはやさしい。積を保つことは

$$bnx \times bny \equiv bn(xy) \bmod mn$$

を言えばよい。両辺を n で割って

$$bxbny \equiv b(xy) \bmod m$$

を言えばよいが $bn \equiv 1 \bmod m$ によりこれは正しい。したがってこれは環準同型であるが $f([1]_m) = [bn]_{mn} \neq [1]_{mn}$ より単位的環としての準同型ではない。

問題 4.6. S が R の部分環であるとき、埋め込み

$$\iota : S \to R, \quad s \mapsto s$$

は環準同型であることを示せ。

4.3 多項式環

定義 4.3.1. R を可換環とする。t を R とは無関係な文字とする。$R[t]$ によって、R 係数の t を変数とする多項式環を表す。すなわち、$R[t]$ の元は

$$a_n t^n + a_{n-1} t^{n-1} + \cdots + a_1 t + a_0 \quad (a_i \in R)$$

の形のものであり、和と積は通常の計算法則で定義する。

確かめるのが少々面倒なのでここには書かないが、これにより $R[t]$ は可換環となる。$a_1, \ldots, a_n$ が 0 であるような多項式を定数と言う。これにより、$R \subset R[t]$ とみなすことができる。$R[t]$ における 0 は定数 0 である。0 以外の元 $f(t)$ は $f(t) = a_n t^n + a_{n-1} t^{n-1} + \cdots + a_1 t + a_0$ $(a_i \in R)$, $a_n \neq 0$ の形に書ける。このとき、n を f の次数 (degree) といい、$\deg(f)$ であらわす。0 の次数は $-\infty$ とするのが普通である。

R が単位的可換環であるとき、$R[t]$ は定数 1 を積の単位元とする単位的可換環である。

二変数多項式環 $R[x, y]$ も同様に定義される。その元は、$\sum a_{n,m} x^n y^m$ の形の元である。

問題 4.7. $S := R[x]$ とおくと、

$$S[y] = R[x][y]$$

と $R[x, y]$ は環同型であることを示せ。

これは、例えば

$$ax^2 + bxy + cy^2 + ex + fy + g = cy^2 + (bx + f)y + (ax^2 + ex + g)$$

という具合に二変数多項式を一つの文字について整理することができるということを意味している。

4.4　生成

一般に、代数構造の与えられた集合 S において、「$T \subset S$ が生成する S の部分代数構造」といったら T を含む（包含関係に関して）最小の S の部分代数構造を指す。

具体的にいう。例えば $\mathbb{C}$ において、$z \in \mathbb{C}$ の生成する単位的部分環 R はどんなものだろうか。単位的部分環であることから、$0, 1 \in R$ である。加法群であるから、$1+1+1, -1-1$ などは全て R に入り、$\mathbb{Z} \subset R$ となる。$z \in R$ より $a \in \mathbb{Z}$ に対して $az \in R$。また $z^2, z^3, \ldots, \in R$。こうして、整数係数の z の多項式の形に書ける元は全て R に入る。

$$\{\sum_n a_n z^n | a_i \in \mathbb{Z}\} \subset R.$$

しかるに、左辺はすでに単位的可換環になっている。ということは、これが z を含む最小の単位部分環である。

定義 4.4.1. 上の環を $\mathbb{Z}[z]$ であらわす。これは $\mathbb{C}$ の単位的部分環であって、z を含むもののうち最小のものである。

注意 4.4.2. t を変数とする多項式環 $\mathbb{Z}[t]$ と同じ記法でまぎらわしいが、多項式環 $\mathbb{Z}[t]$ と z が生成する単位的部分環 $\mathbb{Z}[z]$ とは似て非なるものである。前者においては t はただの文字であり、後者においては z はある環の元である。

例 4.4.3. 上で、z が $i := \sqrt{-1}$ であるときの $\mathbb{Z}[z] \subset \mathbb{C}$ を求めよう。$z^2 = -1$, $z^3 = -z$, $z^4 = 1$,... であるから、z の多項式は一次式に書き換えられる。よって

$$\mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{Z}\}.$$

この環を、ガウスの整数環という。

定義 4.4.4. R を単位的環とする。単位的環 S が R 代数 (R-algebra) であるとは、ある単位的環準同型 $\rho : R \to S$ が定まっていること。つまり、厳密には (S, ρ) の組を R 代数という。

定理 4.4.5. (S, ρ) を R 代数とし、$R[t]$ を多項式環とする。$s \in S$ を S の元で、$\rho(R)$ の各元と可換なものとする。このとき、$f(t) \in R[t]$ の係数を一斉に ρ で変換したものを $\rho(f) \in S[t]$ と書き、そこで t に s を代入して得られた式を $\rho(f)(s) \in S$ とあらわす。

$$\phi : R[t] \to S, \quad f(t) \mapsto \rho(f)(s)$$

は単位的環準同型となる。$\phi(t) = s$, $\phi|_R = \rho$ となる、ただ一つの単位的環準同型である。

ϕ の像は、S において $\rho(R)$ と s が生成する単位的部分環に他ならない。

問題 4.8. 上の定理を証明せよ。

証明する代わりに、例を挙げておく。ほとんどの場合、$R \subset S$ である。このとき、ρ はこの埋め込みとするのが通常で、無視できる。例えば、$\mathbb{Z} \subset \mathbb{C}$ であり、$z \in \mathbb{C}$ を一つ決めれば

$$\phi : \mathbb{Z}[t] \to \mathbb{C}, \quad f(t) \mapsto f(z)$$

である。これは先に考えたものである。

例 4.4.6. R を単位的可換環とし、$S := M_n(R)$ を行列環とする。$\rho : R \to S$ を $a \mapsto aI_n$ で定めると単位的環準同型となる。いま、行列 $A \in M_n(R)$ を一つ選ぶと、上のように

$$\phi : R[t] \to M_n(R), \quad t \to A$$

が唯一つ定まる。(R が可換環であるので、A と $\rho(R) =$ スカラー行列の集合 は可換である。)

例えば、

$$\phi : f(t) = at^2 + bt + c \mapsto aIA^2 + bIA + cI = aA^2 + bA + cI$$

である。右辺を $f(A)$ と書くことは線形代数学で習っていると思う。$R[A] \subset M_n(R)$ なる単位的部分環が定義される。

問題 4.9. $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ とおく。ガウスの整数環 $\mathbb{Z}[i]$ と $\mathbb{Z}[A] \subset M_2(\mathbb{Z})$ が環同型であることを示せ。

4.5 整域と体

以後体といったら特に断らない限り可換体を表すことにする。

定義 4.5.1. R を環とする。$ab = 0$ となるような $b \neq 0$ が存在する R の元 a を零因子 (zero divisor) という。

0 以外の零因子を持たない単位的可換環を整域 (integral domain) という。ただし、零環は整域とは考えない。

問題 4.10. 単位的可換環 R に対し、R が整域であることと、$R - \{0\}$ が $(R, 1, \cdot)$ の部分モノイドであることが同値であることを示せ。

命題 4.5.2. 体は整域である。

証明. R を体とする。a を零因子とすると、$b \neq 0$ に対して $ab = 0$。体なので b^{-1} が存在する。これを両辺にかけると $a = abb^{-1} = 0b^{-1} = 0$。ここに、最後の等式は 4.1 より得られる。 □

問題 4.11. 整域の単位部分環は整域であることを示せ。

問題 4.12. R が整域とする。$a, x, y \in R$ で $a \neq 0$ のとき、

$$ax = ay \Rightarrow x = y$$

がいえることを示せ。

例 4.5.3.　1. $\mathbb{Z}$ は体ではないが整域である。

2. $m, n \geq 2$ とするとき $\mathbb{Z}/mn$ は整域でない。$[m] \cdot [n] = [mn] = [0]$ だから。

問題 4.13. 単位的可換環 R が整域であることと、全ての $a \in R - \{0\}$ に対し加法群の準同型

$$L_a : R \to R, \quad x \mapsto ax$$

が単射であることとが同値であることを示せ。(ヒント:系 2.4.71。)

問題 4.14. 単位的可換環 R が体であることと、全ての $a \in R - \{0\}$ に対し (上で定義した) L_a が全射であることとが同値であることを示せ。(ヒント:全射であることと、像が 1 を含むこととが同値になることを示せ。)

問題 4.15. 有限整域 (台集合が有限集合であるような整域) は体であることを示せ。

命題 4.5.4. R を可換環とし、$f, g \in R[t]$ を多項式とする。このとき

$$\deg(f \cdot g) \leq \deg(f) + \deg(g).$$

R が整域なら等号が成立する。$\deg(1) = 0$ より

$$\deg : (R[t], \cdot, 1) \to (\mathbb{N} \cup \{0, -\infty\}, +, 0)$$

なるモノイド準同型となる。

証明. f の次数が n, g の次数が m とする。それぞれの最高次の項は $a_n t^n$, $b_m t^m$ $(a_n, b_m \neq 0)$ である。もし R が整域ならば $a_n b_m \neq 0$ なので fg の最高次の項は $(a_n b_m) t^{n+m}$ となり、その次数は $n+m$ である。よって後半が成り立つ。前半に関しては、R が整域でなければ $a_n b_m = 0$ の可能性があるが、なんにせよ $n+m$ を超えた次数の項はあらわれないので不等号がなりたつ。

f, g のいずれかが 0 である場合もうまく行く。$\deg(0) = -\infty$, $-\infty + n = -\infty$ と定義すればよい (行き先はモノイドである、§2.4.10 の最後の方に説明がある)。各自確かめよ。 □

4.6　イデアル

4.6.1　環の構造と同値関係

定理 4.6.1. (同値関係による剰余環) R を (単位的とは限らない、非可換かも知れない) 環とする。$\sim$ を R(の台集合) 上の同値関係とする。

商写像

$$q : R \to R/\sim$$

が環準同型となるような和、積が $R/\sim$ に定義される必要十分条件は、$\sim$ が和、積とコンパチブルであること、すなわち任意の x_1, x_1', x_2, x_2' に対して

$$x_1 \sim x_1', x_2 \sim x_2' \Rightarrow x_1 + x_2 \sim x_1' + x_2', \;\; x_1 \cdot x_2 \sim x_1' \cdot x_2'$$

が成立することである。

R が単位的環である場合にも、この条件が満たされれば $R/\sim$ には $\bar{1}$ を単位元とする単位的環の構造が入り、q は単位的環の準同型になる。

証明. 十分性：商群の定理 2.4.24 により $R/\sim$ は加法群であり、q は群準同型になる。商半群の定理 2.2.11 により $R/\sim$ は積に関する半群となり、q は半群準同型となる。あとは $R/\sim$ が環になることさえ言えばよい。分配法則の成立を言えばよい。q は全射だから

$$q(a)\cdot(q(b)+q(c))=q(a)\cdot q(b)+q(a)\cdot q(c)$$

を言えば良いが、q が和に関する群準同型、積に関する半群準同型であることから左辺は $q(a\cdot(b+c))$, 右辺は $q(a\cdot b+a\cdot c)$ となり、R において分配法則がなりたつことからこれらは等しい。左右入れ替えた分配法則についても同様である。

単位的可換環に関しては、商半群の定理を商モノイドの定理 2.3.20 にすりかえればよい。(定理 2.4.30 の言葉で言うなら、分配法則や単位元の法則は無条件等号型なので、商代数に遺伝する。)

必要性：商群の定理 2.4.24 により和と $\sim$ はコンパチブル。商半群の定理 2.2.11 により積と $\sim$ はコンパチブル。 □

4.6.2 イデアル

群 $(G,\circ,e)$ において、演算 $\circ$ とコンパチブルな同値関係 $\sim$ は、ある正規部分群 $N\triangleleft G$ による合同関係 $\sim_N^L$ (正規部分群の時は $\sim_N^R$ としても同じ) としてあらわされ (定理 2.4.75)、商群 $G/\sim = G/N$ を定義した。このとき、$\sim$ から N を作るには

$$N:=[e]_\sim=\{g\in G|g\sim e\},$$

N から $\sim$ を思い出すには

$$a\sim b\Leftrightarrow a\circ b^{-1}\in N$$

とおけば良いのであった。

環 R の場合に、同様の考察をしてみよう。全ての演算とコンパチブルな同値関係 $\sim$ とは、$+,\cdot$ とコンパチブルな同値関係に他ならない。今、積 $\cdot$ のことをしばらく無視すると、$(R,+,0)$ は可換群であり、$\sim$ はその演算 $+$ とコンパチブルであるから上の事実よりある正規部分群 $I\triangleleft R$ が存在して

$$a\sim b\Leftrightarrow a-b\in I$$

が成立する。そして、

$$I=\{r\in R|r\sim 0\}$$

となる。

$(R,+,0)$ は可換群なので、正規部分群と部分群は同じ概念である。では、いつ部分群 I が与える二項関係 $\sim_I$:

$$a\sim_I b\Leftrightarrow b-a\in I$$

は積 $\cdot$ についてもコンパチブルになるだろうか。結論から言えば、I が両側イデアルであることが $\sim_I$ が和と積とコンパチブルである必要十分条件なのである。

定義 4.6.2. (イデアル) R を環とし、$I \subset R$ を加法に関する部分群とする。I が左側イデアル (left ideal) であるとは、I の元に左から R のどの元をかけても I の中に留まること、すなわち

$$\forall a \in R, a \cdot I \subset I$$

が成り立つこと。I が右側イデアル (right ideal) であるとは、

$$\forall a \in R, I \cdot a \subset I$$

が成り立つこと。I が両側イデアル (both-side ideal) であるとは、左側イデアルでありかつ右側イデアルであること。（可換環においては、この三つのイデアルの概念は全て等しい。この時は単にイデアルという。）

問題 4.16. R を単位環とする。$I \subset R$ がイデアルである必要十分条件は、

1. $0 \in I$,
2. $\forall a, b \in I, (a + b \in I)$,
3. $\forall r \in R, \forall a \in I, (r \cdot a \in I)$,

の三つが成り立つことであることを示せ。

定理 4.6.3. R を環とし、$\sim$ を R（の台集合）上の同値関係とする。

$$I_\sim := [0]_\sim = \{x \in R | x \sim 0\}$$

とおく。$\sim$ が R の積、和とコンパチブルである必要十分条件は、$I_\sim$ が両側イデアルであることである。

逆に、$I \subset R$ が両側イデアルであるとき、

$$a \sim_I b \Leftrightarrow a - b \in I$$

で二項関係 $\sim_I$ を定めると、これは R 上の同値関係であり積、和とコンパチブルである。

$\sim \mapsto I_\sim$ は、

$$\{R \text{ 上の積和とコンパチブルな同値関係の集合 }\} \to \{R \text{ の両側イデアルの集合 }\}$$

なる一対一対応を与える。その逆写像は $I \mapsto \sim_I$ で与えられる。

証明. $\sim$ を和とコンパチブルな同値関係とすると、定理 2.4.75 より $I_\sim$ は加法群 R の部分群である。今、$x \in I_\sim$ とすると $x \sim 0$。$\sim$ が積についてコンパチブルとすると、

$$a \cdot x \sim a \cdot 0 \overset{\text{問題 } 4.1}{=} 0.$$

よって $a \cdot x \in I_\sim$、すなわち $I_\sim$ は左側イデアル。左右を入れ替えて、右側イデアルでもある。これで、

$$\text{「}\sim \text{ が和積とコンパチブル} \Rightarrow I_\sim \text{ は両側イデアル」}$$

が言えた。逆に、I が両側イデアルなら $\sim_I$ が和積とコンパチブルであることも、同じくらいの手間で示せる。読者に任せる。 □

問題 4.17. 定理 4.6.3 の証明を完成させよ。

定義 4.6.4. R を環、I をその両側イデアルとする。$a, b \in R$ に対し二項関係 $a \equiv b \bmod I$ を

$$a \equiv b \bmod I \Leftrightarrow a - b \in I$$

で定義すると、これは同値関係 $\sim_I$ と一致する。I を法とする合同関係という。

例 4.6.5. (単項イデアル) R を可換環とし、$a \in R$ とする。R の部分集合 (a) を

$$(a) := \{r \cdot a | r \in R\}$$

と定義すると、これはイデアルとなる。a が生成する単項イデアル (principal ideal) という。
要は、a の倍数のつくる集合を (a) と書く。

問題 4.18. 上の例で、(a) がイデアルとなることを示せ。実は、R が可換環でなくても (a) は左側イデアルになることを示せ。

例 4.6.6. $m \in \mathbb{Z}$ とするとき、定義 1.3.24 で定義した同値関係 $x \equiv y \bmod m$ は定義 4.6.4 において $I = (m)$ としたもの $x \equiv y \bmod (m)$ と一致する。

4.6.3 環準同型定理

定理 4.6.7. (イデアルによる剰余環) R を環とし、I を両側イデアルとする。

$$q : R \to R/I$$

が環準同型となるような和、積が R/I にただ一通り定義される。この R/I を R の I による剰余環 (residue ring) と言う。q を剰余準同型 (residue homomorphism, residual homomorphism) と言う。

証明. 定理 4.6.3 と定理 4.6.1 から従う。 □

剰余とは、「割った余り」の意味である。今、例 4.6.6 で見たように $R = \mathbb{Z}$, $I = (m)$ とすると

$$R/I = \mathbb{Z}/(m)$$

は、

$$\mathbb{Z} \text{ を } x \sim y \Leftrightarrow x - y \in (m) \text{ という同値関係で類別したもの}$$

に他ならない。これは定義 1.3.27 で定義した $\mathbb{Z}/m$ に一致する。すなわち、前章までの $\mathbb{Z}/m$ は $\mathbb{Z}/(m)$ なる剰余環である。

$\mathbb{Z}/m$ は「整数を m で割った余りの全体」と同一視されるので、「剰余環」の名前がある。

定義 4.6.8. (核、カーネル）$f : R_1 \to R_2$ を環準同型とする。その核 (Kernel) を

$$\mathrm{Ker}f := \{x \in R_1 | f(x) = 0_2\}$$

で定義する。すなわち、R_2 の零元の f による逆像のことである。

命題 4.6.9. 上の定義 4.6.8 で、$\mathrm{Ker}f$ は R_1 の両側イデアルである。

証明. 問題 4.16 を用いて直接証明すれば易しい。（もっと哲学的な証明は、注 2.4.34 を使って得られる。環の公理は無条件等号型なので、$\sim_f$ は R_1 に指定された環の演算とコンパチブルであり、したがって定理 4.6.3 より $[0]_{\sim_f}$ は両側イデアルである。これは $\mathrm{Ker}f$ に他ならない。） □

問題 4.19. 上の命題を証明せよ。

定理 4.6.10. R を環とし、I を R の両側イデアルとする。$q : R \to R/I$ を剰余準同型とする。$f : R \to S$ を任意の環準同型とする。

環準同型 $h : R/I \to S$ であって、

$$f = h \circ q$$

なる性質をもつものが存在する必要十分条件は、

$$I \subset \mathrm{Ker}f$$

となることである。このとき、h はただ一つに決まる（しばしば $\bar{f}$ で表される。）

この状況を $\bar{f}$ が well-defined であるという。

証明. 群の場合の対応する定理 2.4.77 の証明とほぼ同じである。違うのは、加法に関する群準同型 $\bar{f}$ が環準同型にもなることを示さなくてはならないところだけである。これは

$$\bar{f}([x]_I \bar{\cdot} [y]_I) = \bar{f}([x \cdot y]_I) = f(x \cdot y) = f(x) \cdot f(y) = \bar{f}([x]_I) \cdot \bar{f}([y]_I)$$

から従う。 □

例 4.6.11. §3.3 で

$$q_m^- : \mathbb{Z}/(mn) \to \mathbb{Z}/m$$

なる群準同型を作ったが、これは環準同型でもある。上の定理 4.6.10 において、$R = \mathbb{Z}$, $S = \mathbb{Z}/m$, $f : \mathbb{Z} \to \mathbb{Z}/m$ を剰余準同型とし、$I := (mn)$ とする。

$$\bar{f} : R/I = \mathbb{Z}/(mn) \to S = \mathbb{Z}/m$$

なる環準同型が定義されるには、

$$I = (mn) \subset \mathrm{Ker}f = (m)$$

が示されれば良い。これは単に、「mn の倍数はどれも m の倍数である」という自明な事実である。

定理 4.6.12. (環の準同型定理) R, S を環とし、$f : R \to S$ なる環準同型が与えられたとする。$f(R) \subset S$ で f による R の像を表す。このとき、

1. $f(R)$ は S の部分環である。
2. $I := \mathrm{Ker}f$ は R の両側イデアルで、$\sim_I$ は R の和、積とコンパチブルな同値関係である。
3. f が
$$R \xrightarrow{q} R/I \xrightarrow{\bar{f}} S$$
なる合成となるような $\bar{f}$、すなわち
$$f = \bar{f} \circ q$$
なる $\bar{f}$ がただ一つ存在する。そして、その終集合を $f(R)$ に制限して得られる
$$\bar{f} : R/I \to f(R)$$
は環同型となる。

証明. 群の場合の定理 2.4.78 と同様に証明できる。 □

例 4.6.13. R を単位的環とすると、命題 4.2.6 により単位的環準同型 $f : \mathbb{Z} \to R$, $1_{\mathbb{Z}} \mapsto 1_R$ が存在する。$\mathrm{Ker}f$ は $\mathbb{Z}$ のイデアルであるが、ある整数 $m \geq 0$ により $\mathrm{Ker}f = (m)$ となることが示せる（単項イデアル整域、次章参照）。

こうして、$f(\mathbb{Z}) \subset R$ は $\mathbb{Z}/m$ と同型になることが示される。

問題 4.20. 上の事実「$\mathrm{Ker}f = (m)$ となる m が存在する」を証明せよ。（参考：定理 2.4.56 の証明。）

例 4.6.14. $R := \mathbb{R}[t]$ とし、環準同型
$$f : \mathbb{R}[t] \to \mathbb{C}, \quad g(t) \mapsto g(\sqrt{-1})$$
を考える。
$$\mathrm{Ker}f = \{g(t) \in \mathbb{R}[t] | g(\sqrt{-1}) = 0\}$$
である。因数定理から、
$$g(t) \in \mathrm{Ker}f \Leftrightarrow t - \sqrt{-1} | g(\sqrt{-1})$$
である。実多項式 $g(t)$ が解 $\sqrt{-1}$ を持つなら、その複素共役である $-\sqrt{-1}$ も解である。よって、$g(t)$ は $(t - \sqrt{-1})(t + \sqrt{-1}) = t^2 + 1$ で割り切れる。逆に、$t^2 + 1$ で割り切れるような多項式 $h(t)$ は、$\pm\sqrt{-1}$ を解に持つので $h(\sqrt{-1}) = 0$、すなわち $h \in \mathrm{Ker}f$。以上をあわせると
$$\mathrm{Ker}f = (t^2 + 1)$$
となる。環準同型定理によれば、
$$\mathbb{R}[t]/(t^2 + 1) \to \mathbb{C}, \quad t \to \sqrt{-1}$$
なる環の同型が得られる。

例 4.6.15. $\mathbb{R}[t]/(t^2+1)$ で、t の属する同値類を $[t]$ と書く代わりにもう t と書いてしまうことにする。$\mathbb{R}[t]/(t^2+1)$ において計算をすることは、和積差の計算を多項式でしておいて、結果をいちいち t^2+1 で割った余りをとるという計算をすることになる。例えば、$t^2 = (t^2+1) - 1 \equiv -1 \bmod (t^2+1)$ であるので、t は $\sqrt{-1}$ の役割を果たす。

例 4.6.16. 単項でないイデアルも存在する。$\mathbb{R}[x,y]$ で、実係数二変数多項式環を表す。

$$(x,y) := \{f(x,y)x + g(x,y)y | f,g \in \mathbb{R}[x,y]\} \subset \mathbb{R}[x,y]$$

とおくと、これは $\mathbb{R}[x,y]$ のイデアルとなる。もしこのイデアルが単項イデアルであったとすると、

$$(x,y) = (a(x,y))$$

なる多項式 $a(x,y)$ が存在するはずである。左辺には x, y が含まれるから、x は $a(x,y)$ の倍多項式であり、y も $a(x,y)$ の倍多項式である。しかし、そのような $a(x,y)$ は定数しか存在せず、上の等号は成り立たない。

問題 4.21. 上の、(x,y) が単項イデアルではないという事実の証明を詳細に述べよ。

4.6.4　倍元、約元、単元、既約元

R を可換環とする。$a,b \in R$ に対して、

$$ax = b$$

となる $x \in R$ が存在するとき、b は a の倍元または倍数（multiple）といい、a は b の約元または約数 (divisor) という。a が b を割り切るともいう。

$$a|b$$

であらわす。

$$a \cdot 0 = 0$$

より、0 は全ての元の倍数であり、全ての元は 0 の約数である。

問題 4.22. b が a の倍数であることと、$b \in (a)$ であることが同値であることを示せ。

問題 4.23. b が a の倍数であることと、$(b) \subset (a)$ であることが同値であることを示せ。

R を単位的可換環とする。$R^\times$ で R の積に関する可逆元の集合を表す。積に関する可逆元のことを単元 (unit element) ともいう。

問題 4.24. $a \in R$ が可逆元であることと、a が 1 の約数であることが同値であることを示せ。

問題 4.25. R を単位的可換環とする。$a \in R$ が可逆元であることと、$R = (a)$ であることが同値であることを示せ。

問題 4.26. 可逆元を含むイデアルは R 自身となることを示せ。

問題 4.27. R を整域とする。$a,b \in R$ に対し、

$$(a) = (b) \Leftrightarrow \exists u \in R^\times (au = b)$$

を示せ。

定義 4.6.17. 単位的可換環 R において、$a \in R$ が既約元 (irreducible element) であるとは a の約元が自明なものに限られることである。すなわち、$xy = a$ ならば x か y が積の可逆元（すなわち単元）となることを言う。

ただし、0 は既約元とみなさない。

$xy = a$ ならば $x = a$ または $y = a$ と書きたいところだが、そうは問屋がおろさない。$(-1)(-a) = a$ であるから。可逆元 u があるとき、$a = u(u^{-1}a)$ だから、可逆元の分、一意には分解され得ない。

問題 4.28. $R = \mathbb{Z}$ とする。R の 0 でない任意の元は、既約元いくつかの積に表わせることをしめせ。

問題 4.29. K を体とし、$R = K[t]$ とする。R の 0 でない任意の元は、既約元いくつかの積に表わせることをしめせ。

4.6.5 素イデアルと整域、素元

R を単位的可換環とし、I をそのイデアルとする。R/I が整域になる条件を考えよう。R/I の任意の二元は $[a], [b]$, $a, b \in R$ と書き表されるから、整域になる必要十分条件を書き下すと

$$[a] \cdot [b] = [0] \Rightarrow [a] = [0] \text{ または } [b] = [0]$$

となる。今、$[x] = [0] \Leftrightarrow x \in I$ であり、$[a] \cdot [b] = [a \cdot b]$ であるから上の条件は

$$a \cdot b \in I \Rightarrow a \in I \text{ または } b \in I$$

となる。

定義 4.6.18. R を単位的可換環、$I \subset R$ をそのイデアルとする。条件

$$\forall a, b \in R, a \cdot b \in I \Rightarrow a \in I \text{ または } b \in I$$

が成立するとき、I を R の素イデアル (prime ideal) という。ただし、$I = R$ は（上の条件を満たしているが）素イデアルと言わない。

注意 4.6.19. $I = R$ のとき、R/I は $[0]$ ただ一個からなる集合であり、かけても足しても $[0]$ しかでてこないものである。このような環を零環という。零環は、整域の定義 4.5.1 からすれば整域にするべきものなのだが、通常は整域とはみなさない。また、体ともみなさない。これにより、$I = R$ は素イデアルとみなさないことと次の定理はマッチしている。

定理 4.6.20. R を単位的可換環、$I \subset R$ をそのイデアルとする。R/I が整域である必要十分条件は、I が素イデアルであることである。

「素イデアル」の「素」は素数 (prime number) の素である。

例 4.6.21. $R = \mathbb{Z}$ とする。$a \in \mathbb{Z}$ に対し、単項イデアル (a) が素イデアルとなる必要十分条件は a が素数であることである。

証明. (a) が素イデアルである必要十分条件は、

$$xy \in (a) \to x \in (a) \text{ または } y \in (a)$$

となることである。(a) は a の倍数の全体であったから、「xy が a の倍数ならば、x, y のいずれか一つは a の倍数である」ということが成り立つことと、(a) が素イデアルであることとは同値である。a が素数であれば、素因数分解の一意性からこのようなことが成り立つし、a が合成数 $a = mn$ であれば $x = m, y = n$ ととって反例ができる。 □

問題 4.30. 上の証明の詳細を完成させよ。

問題 4.31. 単位的可換環 R のイデアル I が素イデアルである必要十分条件は、$R\backslash I$（R から I の元をとりさった残り）が $(R, \times, 1)$ の部分モノイドであることを示せ。

定義 4.6.22. (素元) R を単位的可換環とする。$a \in R$ が素元であるとは、(a) が素イデアルであること。言い換えると、

1. a は可逆元ではなく、かつ
2. $xy = az$ なる $x, y, z \in R$ が存在するとき x または y が a で割り切れること。

（a が可逆元なら $R = (a)$ であり、R 自身は素イデアルと言わないのであった。）

R が整数環のとき、素元の全体は素数 (に符号 $\pm$ をつけたもの) の全体と一致する。

問題 4.32. R を単位的可換環とする。R が整域である必要十分条件は、(0) が素イデアルであることである。

注意 4.6.23. ここで注意するのは早計だが、松坂和夫の参考書 [2] における素元の定義は、このノートにおける「可逆元でない既約元」になっている。しかし、現代的には「素元」と「可逆でない既約元」は区別しないとならない。この辺の事情は §4.7 で再び触れる。

4.6.6　極大イデアルと体

定義 4.6.24. R を単位的可換環、I をそのイデアルとする。I を含む R のイデアルが I 自身か R しか存在しないとき、I を極大イデアル (maximal ideal) という。

ただし、上の条件を満たしているが R 自身は極大イデアルとは言わない。

定理 4.6.25. R を単位的可換環、I をそのイデアルとする。R/I が体である必要十分条件は、I が極大イデアルであることである。

証明. R/I が体であるとして、I が極大イデアルであることを示す。I より真に大きな R でないイデアル $I \subset J \subset R$ $(J \neq I, \neq R)$ が存在したとする。$x \in J, x \notin I$ を持ってくる。$x \notin I$ だから $[x] \in R/I$ は $[0]$ でない。R/I は体だから $[x]$ は可逆、すなわちある $[y] \in R/I$ があって $[x][y] = [1]$ となる。$[] : R \to R/I$ は環準同型 (定理 4.6.7 の q が $[]$) だから $[0] = [x][y] - [1] = [xy - 1]$。言い換えると $xy - 1 \in I$ である。$x \in J$ より $xy \in J$。J は加法群だから $1 = xy - (xy - 1) \in J$。よって任意の $r \in R$ に対し $r = r \cdot 1 \in J$。すなわち $R \subset J$。$J \subset R$ は常に正しいので $J = R$。これは矛盾。よって I は極大イデアルである。

次に、I が極大イデアルであると仮定して R/I が体であることを示す。R/I の 0 でない元を持ってくる。$x \in R$ により $[x]$ と書ける。これが可逆であることを示せばよい。$[x] \neq [0]$ であるから $x \notin I$。ここで I と x で生成される R のイデアル $I + (x) = \{a + cx | a \in I, c \in R\}$ を考える。I の極大性から $I + (x) = R$ である。特に、$a + cx = 1$ となる $a \in I, c \in R$ があることになる。すると $[a]_I = [0]_I$ より

$$[1] = [a + cx] = [a] + [cx] = [cx] = [c][x].$$

これは $[x] \in R/I$ が可逆であることを示している。 □

次の命題は、なかなか証明が難しい。

命題 4.6.26. R を単位的可換環とし、I を $I \neq R$ なるイデアルとする。すると、I を含む極大イデアルが R に存在する。

問題 4.33. R の R 自身ではないイデアルの集合を

$$\mathcal{I} := \{J \subset R | J\text{:イデアル}, J \neq R\}$$

とする。

1. $\mathcal{I}$ が、包含関係について帰納的順序集合（[1] 参照）であることを示せ。
2. Zorn の補題（[1] 参照）により、任意の $I \in \mathcal{I}$ に対してそれを含む極大イデアルが存在することを示せ。

4.7 単項イデアル整域

4.7.1 整数環の素因数分解の一意性

整数論において基本的でかつ結構難しいのは、素因数分解の一意性である。例えば、2^n が 3 で割り切れないことはよく知られている。

$$2^n = 3x$$

とすると、右辺で x を素因数分解することで素因数 3 を含んだ分解が得られるが、左辺には 3 は現れないから素因数分解が二通りあることになり矛盾である。

この証明には、「自然数は素数の積にかける。その表し方はただ一通りである。」という定理、すなわち「素因数分解の一意性」が使われている。しかし、なぜ素因数分解はただ一通りなのか？中高の数学の教科書は、これについて証明を与えていないものが多い。

整数環において素因数分解がただ一通りなのは、つきつめれば次の定理による。

定理 4.7.1. $\mathbb{Z}$ において、可逆でない既約元は素元である。

なんのことだかは、以下に説明する。

単位的可換環 R における素元 a とは、$a \in R$ であって (a) が素イデアルとなるもののことであった。これは、$x, y, z \in R$ に対して

$$xy = az \Rightarrow (\exists b \in R, x = ba) \text{ または } (\exists c \in R, y = ca)$$

が成り立つことであった。（定義 4.6.22。）
　既約元の方も復習しておく (定義 4.6.17)。

定義 4.7.2. 単位的可換環 R において、$a \in R$ が既約元 (irreducible element) であるとは a の約元が自明なものに限られることである。すなわち、$xy = a$ ならば x か y が積の可逆元（すなわち単元）となることを言う。
　ただし、0 は既約元とみなさない。

問題 4.34. R が整域の時は、$a \in R$ が既約元であることは $a \neq 0$ で

$$xy = a \Rightarrow (\exists b \in R, x = ba) \text{ または } (\exists c \in R, x = ca)$$

がなりたつことと同値であることを示せ。

　次の定義は実質的に中学か高校で習うものである。

定義 4.7.3. $\mathbb{Z}$ において、可逆でない既約元のうち正のものを素数 (prime number) という。

　これで、定理 4.7.1 に現れた既約元、素元の定義が明らかになった。

命題 4.7.4. 整域 R において、素元は既約元である。

証明. 素元ならば、問題 4.34 の条件を満たす。とくに $z = 1$ でもこの条件を満たす。これが、a が既約元であることに他ならない。 □

　では、定理 4.7.1 がなぜ素因数分解の一意性を導くのか。そもそも素因数分解の一意性とは何か。

定義 4.7.5. 単位的可換環 R において、二つの元 a, b が同値であるとは、$a = ub$ となる単元 $u \in R^\times$ があること。このとき $a \sim b$ であらわす。

問題 4.35. R が整域であるとき、上の条件は、二つの単項イデアルが一致すること

$$(a) = (b)$$

と同値であることを示せ。

定理 4.7.6. $x \in \mathbb{Z}$ とし、$x \neq 0$ とする。$\mathbb{Z}$ の 1 でない互いに同値でない素元 $p_1, p_2, \ldots, p_s$ と自然数 $n_1, n_2, \ldots, n_s$ (> 0) が存在して

$$x = up_1^{n_1} p_2^{n_2} \cdots p_s^{n_s}$$

と書けたとする（ここに $u = \pm 1$）と、このような書き方は ± 1 倍を除いてただ一通りである。すなわち、他に

$$x = vq_1^{m_1} q_2^{m_2} \cdots q_t^{n_t}$$

とかけたとする（v は ± 1、q_i は相異なる既約元）と、$s = t$ で q_i の番号を入れ替えれば $\pm p_i$ と一致し $m_i = n_i$ となる。

証明. p_1 は素元であるから、$p_1|x = vq_1^{m_1}\cdots q_t^{n_t}$ より $p_1|v$ または $p_1|q_1$ または ... または $p_1|q_t$。$p_1|v$ とすると、可逆元の約数は可逆元だから p_1 が素元であることに反する。よって p_1 は q_i のいずれかの約数。q の添え字をとりかえることにより $p_1|q_1$ としてよい。q_1 は既約元なので $p_1 = \pm q_1$ である。よって

$$up_1^{n_1}p_2^{n_2}\cdots p_s^{n_s} = vq_1^{m_1}q_2^{m_2}\cdots q_t^{n_t}$$

であり、両辺を $p_1 = \pm q_1$ で割ること（問題 4.12）で

$$up_1^{n_1-1}p_2^{n_2}\cdots p_s^{n_s} = (\pm v)q_1^{m_1-1}q_2^{m_2}\cdots q_t^{n_t}$$

これを次々繰り返していけば、$p_1 = \pm q_1$ は同時につきるはずである。なぜならば、もしもどちらか片方が先に尽きたとして、かりに q_1 が先に尽きたとする。p_1 は左辺に残っているから、この証明の先頭に書いた議論により p_1 は $q_2, \ldots, q_t$ のいずれかを割り切り、（q_i の既約性から）割り切ったものと同値となる。しかるに、p_1 と q_1 は同値であるから、$q_1, q_2, \ldots, q_t$ のいずれも同値ではない、という仮定に反している。

こうして次々に既約元をキャンセルしていくことで、このような分解は ± 1 倍と積の順序の入れ替えを除いてただ一通りであることがわかる。

x が可逆元であるときには、$s = 0$ として上の定理は成立しているものとみなす。 □

定理 4.7.7. $\mathbb{Z}$ の全ての 0 でない元 x に対し、x は既約元の積としてあらわされる。

証明. x が既約元でないとする。$x = yz$ （y, z は単数でない）という形にできる。すると、$|y|$,$|z|$ は $|x|$ より真に小さい。$|x|$ に関する帰納法を使う。$|x| = 1$ では $x = \pm 1$ より 0 個の既約元の積としてあらわされる。$|x| \leq n-1$ ならば既約元の積に分解される、と仮定して $|x| = n$ の時を証明すればよい。が、$x = yz$ より y、z の既約分解は帰納法の仮定により存在するのでそれらを合わせたものが x の既約分解である。 □

以上により、「整数はすべて素数の積に分解され、その分解の仕方は一意である」という定理が証明された。ただし定理 4.7.1 はまだ証明していないのでその証明を以下に与える。

命題 4.7.8. 整数環では、最大公約数が存在する。すなわち、$a, b \in \mathbb{Z}$ に対して $d|a, d|b$ なる d であって、他に $c|a, c|b$ を満たす c に対しては $c|d$ となるようなものがある。d を $\gcd(a, b)$ と記す。

証明. $am + bn$ の形にかける正の整数のうち、最小のものを d とすると上の性質を満たしている。ということが、定理 2.4.64 の証明に示されている。 □

命題 4.7.9. $a \in \mathbb{Z}$ を可逆でない既約元とすると、それは素元である。

証明. $az = xy$ とする。$\gcd(a, x)|a$ であり、a は既約元だから $\gcd(a, x) \sim a$ または $\gcd(a, x) \sim 1$.

前者の時には $a \sim \gcd(a, x)|x$ となるから $a|x$ で、素元の条件を満たす。後者のとき、同様に $\gcd(a, y) \sim a$ ならば $a|y$ で素元の条件を満たす。問題がおきるのは

$$\gcd(a, x) \sim 1, \gcd(a, y) \sim 1$$

のときであるが、このとき

$$an + bx = 1, am + cy = 1$$

が解けるので、辺々掛けて

$$a(anm + ncy + bxm) + bxcy = 1$$

よって定理 2.4.64 より ($aX + (xy)Z = 1$ の形なので)

$$\gcd(a, xy) = 1$$

である。一方 $az = xy$ より

$$a|\gcd(a, xy)$$

であるからこれは矛盾である。 □

4.7.2　多項式環

整数環と同じように、素因数分解の一意性（こういったら、素因数分解が可能であり、かつ分解のしかたが可逆元倍を除いて一意である、ということをさす）が成立するような環として、体係数の多項式環がある。中学・高校の数学で、暗黙のうちに「多項式の因数分解は分解できる限り分解すれば結果はただ一通り」ということを習っている。

整数環と体係数多項式環は、どちらも「余りつき割り算」ができるという点でよく似ている。余りつき割り算ができるような整域のことをユークリッド整域という。先走って言えば、

$$\text{ユークリッド整域} \Rightarrow \text{単項イデアル整域} \Rightarrow \text{素因数分解の一意性が成り立つ整域}$$

となっている。

4.7.3　単項イデアル整域

定義 4.7.10. (単項イデアル整域) 整域 R において、全てのイデアルが単項イデアルとなるとき、R を単項イデアル整域 (principal ideal domain, PID) という。

次の定理は、実質的には定理 2.4.64 の証明で示されている。

定理 4.7.11. 整数環 $\mathbb{Z}$ は単項イデアル整域である。

証明. $I \subset \mathbb{Z}$ をイデアルとする。$I = \{0\}$ ならば $I = (0)$ であり単項イデアルである。そうでないとき、I には 0 以外の元が存在する。$x \in I$ ならば $-x \in I$ だから、正の元が存在する。I に属する正の元のうちで、最小のものを d とする。$d \in I$ より任意の $r \in \mathbb{Z}$ に対して $rd \in I$。よって

$$(d) \subset I$$

である。逆向きの包含関係を示そう。$x \in I$ を持ってくる。x を d で割った余りを考えると

$$x = d \cdot q + r, \quad (0 \leq r \leq d - 1)$$

とできる。ここで、$x \in I, dq \in I$ であるから（I は加法部分群なので）

$$r = x + (-dq) \in I$$

となる。しかるに、d は I の正の元の中で最小のものだったのだから、$r \leq d-1$ が I に入っていることはもし $r > 0$ なら矛盾している。矛盾しないのは、$r = 0$ のときのみである。よって $x = dq \in (d)$ となり、$I \subset (d)$ が言えた。 □

命題 4.7.12. R を単項イデアル整域とし、$a, b \in R$ とする。

$$(a, b) := \{xa + yb | x, y \in R\} \subset R$$

は R のイデアル（a, b の生成するイデアルという）。よって、ある元 d に対して

$$(a, b) = (d)$$

となる。この d を a と b の最大公約数といい、$\gcd(a, b)$ であらわす。d は（その単項イデアルが決まるのだから）可逆元倍を除いて唯一つにさだまる。

$d|a$ かつ $d|b$ が成り立ち、また、$c|a$ かつ $c|b$ ならば $c|d$ である。

証明. 可逆元倍を除いて唯一つに定まることは問題 4.35 からわかる。

最後の部分は、$(d) = (a, b) \supset (a)$ より $d|a$ であり、また $c|a, c|b$ ならば $a, b \in (c)$ でイデアルの性質から $(a, b) \subset (c)$ となることから言える。 □

定理 4.7.13. R を単項イデアル整域とする。

1. ゼロでない元 $x \in R$ は既約元の積に分解する。
2. 可逆でない既約元は素元である。
3. ある元を既約元の積に分解する分解の仕方は、可逆元倍と順序の入れ替えを除いてただ一通りである。

証明. 1. 0 でない元 $a \in R$ を持って来る。既約ならばするべきことはない。いま、a が既約元の積に掛けないとする。すると、a 自身が既約元でないわけだから

$$a = a_1 b_1, \quad a_1, b_1 \notin R^\times$$

と分解する。もし、a_1 が既約元の積にかけて、b_1 が既約元の積にかければ a もそうかけて終わりである。

よって困るのは、すくなくともどちらか一つが既約元の積にかけないときである。必要とあらば入れ替えて、a_1 が既約元の積に掛けないとしてよい。すると、

$$a_1 = a_2 b_2, \quad a_2, b_2 \notin R^\times$$

とできる。そして、a_2 か b_2 か、どちらかは既約元の積にかけない。必要とあらば入れ替えて、a_2 が既約元の積に掛けないとしてよい。

これを続けていくと、$a_1|a, a_2|a_1, a_3|a_2, \ldots$ という無限列ができる。そして、$b_i \notin R^\times$ より、$a_i \sim a_{i+1}$ ではない。すなわち $(a_i) = (a_{i+1})$ ではない。よって、

$$(a) \subset (a_1) \subset (a_2) \subset (a_3) \subset \cdots$$

なる無限列であって、どの $\subset$ も等号ではないものができる。

ここで、合併集合

$$I := \cup_{i=1}^{\infty}(a_i)$$

をとると、これはイデアルになる。和について閉じていること、R の元の積に閉じていることを言わないとならないがいずれも難しくない。

単項イデアル整域の定義から、$I = (x)$ となる x が存在する。$x \in I$ だから、ある j が存在して

$$x \in (a_j).$$

ゆえに $(x) \subset (a_j)$。$(x) = I \supset (a_j)$ は自明だから

$$I = (a_j) \subset (a_{j+1}) \subset \cdots \subset I$$

となり、j より先のイデアルはみな I に等しい。これは矛盾。

2. a を既約元とする。$az = xy$ のとき、$a|x$ か $a|y$ のいずれかが成立することを示せばよい。単項イデアル整域においては最大公約数が上のように定義されるので、命題 4.7.9 の証明がそのまま使えて（可逆でない）既約元は素元となる。

3. 既約元が素元であることがわかれば、定理 4.7.6 の証明と同様にして既約元の積の表し方が可逆元倍を除いて一意であることが示せる。

□

次の定義は、このノートでは使うことがないが可換環論において基礎的なものである。

定義 4.7.14. 単位的可換環 R において、イデアルの列で無限に増大しつづけるもの

$$I_1 \subset I_2 \subset I_3 \subset \cdots$$

（どの $\subset$ も真部分集合）が存在しないとき、R をネーター環（Noetherian ring）という。

上の証明は、単項イデアル整域がネーター環であることを示している。より一般に、ネーター環であることと全てのイデアルが有限生成であることとは同値である。ネーター環の剰余環はネーターであり、ネーター環を係数とする多項式環もネーターである。これらにより、ネーター環上有限生成の環は全てネーターとなる。これらの定理の証明は、「可換環論」と銘打ってある教科書には載っている。

問題 4.36. R がネーター環であることと、R の全てのイデアルが有限生成であることが同値であることを示せ。ここに、イデアル I が有限生成であるとは、ある $x_1, \ldots, x_s \in I$ が存在して

$$I = (x_1, \ldots, x_s) := \{r_1x_1 + r_2x_2 + \cdots + r_sx_s | r_i \in R\}$$

とあらわされることである。

問題 4.37. ネーター環の剰余環はネーターであることを示せ。

問題 4.38. ネーター環を係数とする多項式環はネーターであることを示せ。。

さて、0 でない任意の元が、可逆元倍と順序の入れ替えを除いてただ一通りに素元の積にかけるような整域のことを素元分解一意域 (uniquely factorized domain, UFD) という。上で示したことは、次の定理に他ならない。

定理 4.7.15. 単項イデアル整域は素元分解一意域である。

次の定理も基本的であるが、この授業では取り扱わない。

定理 4.7.16. R を素元分解一意整域とすると、$R[t]$ もそうである。

問題 4.39. 上の定理を証明せよ。(難)

問題 4.40. 素元分解一意整域であるが単項イデアル整域でない環をあげよ。

4.7.4 ユークリッド整域

整数環は単項イデアル整域であった。他に、体係数の多項式環も単項イデアル整域である。

定理 4.7.17. (剰余定理) K を体とし、$f, g \in K[t]$ とする。$g \neq 0$ とするとき、ある $q, r \in K[t]$ が存在して

$$f = gq + r, \quad 0 \leq \deg(r) < \deg(g)$$

となる。

証明. 多項式の割り算の筆算を行えばよい。 □

注意 4.7.18. 上のことは、係数が体でなくても、g の最高次の係数が積について可逆であれば成立する。

問題 4.41. 上の定理を証明せよ。

定理 4.7.19. K を体とするとき、$K[t]$ は単項イデアル整域である。

証明. 定理 4.7.11 の証明とほとんど同様である。イデアル $I \subset K[t]$ を任意にとる。これが単項イデアルであることを示せばよい。$I = \{0\}$ ならば $I = (0)$ で単項イデアル。そうでないとする。$d \in I$, $d \neq 0$ のうちで、$\deg(d)$ を最小にする元を持ってくる。このとき $(d) \subset I$。あとは、

$$I \subset (d)$$

を示せばよい。$f \in I$ を任意にとってくる。剰余定理により

$$f = dq + r, 0 \leq \deg(r) < \deg(d)$$

なる q, r が存在する。$f \in I, d \in I$ より

$$r = f - dq \in I, \quad \deg(r) < \deg(d).$$

d は $\deg(d)$ が最小となる 0 でない I の元としてとったのだから、$\deg(r) < \deg(d)$ と矛盾しないためには $r = 0$ しかない。よって $f \in (d)$, したがって $I \subset (d)$。 □

大体、余りつき除法ができれば単項イデアル整域である。より一般に、ユークリッド整域の概念を導入する。

定義 4.7.20. 順序集合 $(S, \geq)$ が整列集合 (well-ordered set) であるとは、S の任意の空でない部分集合 T に最小元が存在すること。

例 4.7.21. 自然数の集合 $\mathbb{N}$ は普通の順序に関し整列集合である。$\mathbb{N} \cup \{0\}$ や $\mathbb{N} \cup \{-\infty\}$ も整列集合である。

$\mathbb{Z}$ は整列集合でない。$\mathbb{Z}$ 自身（は空でない部分集合である）が最小元を持たないからである。

定義 4.7.22. R を整域とする。R がユークリッド整域であるとは、ある整列集合 V と関数 $v : R \to V$ が存在して、任意の $r \in R$ に対して

$$v(r) = \text{「}V \text{ の最小元」} \quad \Leftrightarrow \quad r = 0$$

および次の「剰余の定理」が成り立つこと。

$$\forall f \in R \forall g \in R, \quad g \neq 0 \quad \Rightarrow \quad \exists q, r \in R \quad f = gq + r, v(r) < v(g).$$

つまり、f を g で割った余り r というべきものが存在して、g より r の方が v で測って小さくなる。

例 4.7.23. $\mathbb{Z}$ においては、$V = \mathbb{N} \cup \{0\}$ とし、$v : \mathbb{Z} \to V$ を $v(x) = |x|$ で定義すればユークリッド整域となる。

$K[t]$ においては、$V = \mathbb{N} \cup \{0, -\infty\}$ とし、$v : K[t] \to V$ を $v(x) = \deg(x)$ で定義すればユークリッド整域となる。

定理 4.7.24. ユークリッド整域は単項イデアル整域である。

問題 4.42. 上の定理を証明せよ。

問題 4.43. ガウスの整数環 $\mathbb{Z}[i] \subset \mathbb{C}$ を考える (例 4.4.3)。$V = \mathbb{N} \cup \{0\}$ とし、

$$v : \mathbb{Z}[i] \to V, z \mapsto z\bar{z} = |z|^2$$

とすると、ユークリッド整域になることを示せ。

したがって、ガウスの整数環はユークリッド整域である。

問題 4.44. $R = \mathbb{Z}[\sqrt{-3}]$ を考える。

$$R = \{a + b\sqrt{-3} | a, b \in \mathbb{Z}\}$$

である。この環の中で、4 は

$$4 = (1 + \sqrt{-3})(1 - \sqrt{-3}) = 2 \cdot 2$$

のように二通りに表される。

1. $1 + \sqrt{-3}, 1 - \sqrt{-3}, 2$ のいずれもが R における既約元であることを示せ。
2. これらのいずれもが素元ではないことを示せ。

よって、R は単項イデアル整域ではない。

4.8 商環、商体

$\mathbb{Z}$ に対して $\mathbb{Q}$ を作る作り方は、例 1.3.17 で述べたとおり

$$(\mathbb{Z} \times \mathbb{N})/\sim,$$

をとることであった。ここに同値関係 $\sim$ は

$$(n, m) \sim (n', m') \Leftrightarrow nm' = n'm$$

で定義する。

同様の構成が、任意の整域 R に対して可能である。

定義 4.8.1. R を整域とする。その商体 (分数体、quotient field, fraction field) $Q(R)$ を、

$$Q(R) := R \times (R - \{0\})/\sim,$$

$$(a, b) \sim (a', b') \Leftrightarrow ab' = a'b$$

で定義する。

(a, b) のことを通常 $\frac{a}{b}$ で表す。$Q(R)$ は通常の通分をする和、分母分子をかける積によって体となる。

証明は、難しくないがだらだらと長い。加法の well-definedness、結合法則、逆元の存在など全部確かめないとならない。一つ一つは簡単である。

問題 4.45. $Q(R)$ に加法・積法が定義されることを示し、体になることを証明せよ。

もう少し一般に、次の定義がある。

定義 4.8.2. R を単位的可換環とする。モノイド $(R, \cdot, 1)$ の部分モノイド S を R の積閉集合という。

定義 4.8.3. R を単位的可換環とし、S を R の積閉集合とする。R の S による商環（分数環, fraction ring of R by S) $S^{-1}R$ を、

$$S^{-1}R := R \times S/\sim,$$

$$(a, b) \sim (a', b') \Leftrightarrow \exists s \in S \quad ab's = a'bs$$

で定義する。(a, b) のことを通常 $\frac{a}{b}$ で表す。

通常の演算により単位的可換環となる。R の S による局所化ともいう。

問題 4.46. R が整域であることと、$S : R - \{0\}$ が積閉集合であることは同値であることを示し、$S^{-1}R = Q(R)$ であることを示せ。

問題 4.47. R が整域とすると、R は $Q(R)$ の部分環とみなせることを示せ。

一般には、$R \to S^{-1}R$ $(r \mapsto \frac{r}{1})$ は単位環準同型だが単射とは限らないことを示せ。

問題 4.48. 上の問題に現れた $\phi : R \to S^{-1}R$ $(r \mapsto \frac{r}{1})$ は次のような性質をもつことを示せ。

任意の単位的環 A と環準同型 $f : R \to A$ に対しても、$f(S) \subset A^\times$ であれば f はある $f' : S^{-1}R \to A$ により $f = f' \circ \phi$ とかける。そのような $f' : S^{-1}R \to A$ は唯一つである。

問題 4.49. 上で、他に $\phi' : R \to R'$ であって、このような性質を持つものがあったとする：

任意の単位的環 A と環準同型 $f : R \to A$ に対しても、$f(S) \subset A^\times$ であれば f はある $f' : R' \to A$ により $f = f' \circ \phi'$ とかける。そのような $f' : R' \to A$ は唯一つである。

このとき、R' と $S^{-1}R$ は環同型であることを示せ。さらに強く、ある環同型 $h : R' \to S^{-1}R$ が存在して $\phi = h \circ \phi'$ となることを示せ。

（ヒント：R' の性質から $R' \to S^{-1}R$, $S^{-1}R$ の性質から $S^{-1}R \to R'$ が存在する。これらの合成が恒等写像になるかどうかだが、これらの合成は ϕ と合成してもかわらず、「そのような f' は唯一つである」という性質から恒等写像に一致する。）

これらの問題により、$R \to S^{-1}R$ はこの性質をもつ唯一つの環と準同型であることがわかる。このような性質は代数学のいたるところに現れ、「普遍性 (universality)」と呼ばれる。

第5章　加群

5.1　環と加群

5.1.1　加群

加法群 $(M,+,0)$ のことを加群 (module) ともいう。

命題 5.1.1. 加法群 M の自己準同型全体 $\mathrm{End}(M)$ は和として関数の和を、積として合成を与えることにより単位的環となる。

これは例 3.4.20 でみたとおりである。

定義 5.1.2. R を環とし、M を加法群とする。環準同型

$$\rho : R \to \mathrm{End}(M)$$

が一つ指定されたとき、M を左 R-加群 (left R-module) という。
R が単位的環のときは、ρ は単位的環準同型であることを要請する。

群の場合を扱った定義 3.4.3 とくらべれば、左 R-加群 M とは「環 R の加法群 M への**環としての作用**が指定されていること」に他ならない。
定理 1.1.30 によれば $\rho : R \to \mathrm{End}(M) \subset \mathrm{Map}(M,M)$ は

$$R \times M \to M, \quad (r,m) \mapsto \rho(r)(m)$$

なる対応を与える。$\rho(r)(m)$ を m に r を作用させた結果といい、

$$r \bullet m := \rho(r)(m)$$

であらわす。のちのち $\bullet$ は省略するが、最初のうちははっきりさせるために書いておく。

問題 5.1. $(R,\cdot,1)$ を単位的環、$(M,+,0)$ を加法群とする。R の M への (左) 作用

$$\bullet : R \times M \to M, \quad (r,m) \mapsto r \bullet m$$

により M が左 R-加群になる必要十分条件は、

1. $r \bullet (m_1 + m_2) = r \bullet m_1 + r \bullet m_2$
2. $(r_1 + r_2) \bullet m = r_1 \bullet m + r_2 \bullet m$
3. $(r_1 \cdot r_2) \bullet m = r_1 \bullet (r_2 \bullet m)$
4. $1 \bullet m = m$

が成り立つことであることを示せ。(それぞれ $\rho(r) \in \mathrm{End}(M)$, ρ が加法を保つこと、ρ が積を保つこと、ρ が単位元を保つこと、を言い換えたものである。)

定義 5.1.3. $(R, \cdot, 1)$ を単位的環、$(M, +, 0)$ を加法群とする。R の M への右作用

$$\bullet : M \times R \to M, \quad (m, r) \mapsto m \bullet r$$

が与えられたとき、この作用により M が右 R-加群になるとは、次の四つを満たすこと。

1. $(m_1 + m_2) \bullet r = m_1 \bullet r + m_2 \bullet r$
2. $m \bullet (r_1 + r_2) = m \bullet r_1 + m \bullet r_2$
3. $m \bullet (r_1 \cdot r_2) = (m \bullet r_1) \bullet r_2$
4. $m \bullet 1 = m$

問題 5.2. M が右 R-加群であることと、環準同型 $R^{op} \to \mathrm{End}(M)$ が与えられていることとが同値であることを示せ。

ここに R^{op} とは、加法群としては R と同じであるが積を

$$r \cdot_{R^{op}} r' := r' \cdot_R r$$

で定義した環である。

R が可換環のときには $R = R^{op}$ であるから左 R 加群と右 R 加群は同じ概念となる。この時は単に R-加群という。

定義 5.1.4. R が体のとき、R-加群を R 線形空間という。

線形代数の教科書を調べて、線形空間の定義が「加法群であること、および問題 5.1 の 4 つの公理を満たすこと」であることを確認してみてほしい。

問題 5.3. 環 R は、左 (右) から R の元をかけることにより左 (右)R 加群であることを示せ。

定義 5.1.5. 左 R 加群 M に対し、その R 部分加群 N とは (1) 部分加法群であって (2) R の作用に閉じているもの。すなわち

1. $m_1, m_2 \in N \Rightarrow m_1 + m_2 \in N$, さらに　$0 \in N$
2. $r \in R, n \in N \quad \Rightarrow \quad r \bullet n \in N$

となるもの。

問題 5.4. R の部分集合 S が左 R 部分加群であることと、S が R のイデアルであることが同値であることを示せ。

以下、R 加群といったら左 R 加群を指すものとする。

定義 5.1.6. R を単位的環とし、M_1, M_2 を R-加群とする。M_1 から M_2 への R-加群としての準同型とは加法群の準同型

$$f : M_1 \to M_2$$

であって、R の作用と「可換」なもの。すなわち

$$f(r \bullet_1 m) = r \bullet_2 f(m)$$

が全ての $r \in R, m \in M_1$ について成り立つこと。

さらに f が逆写像を持ち、それが R-加群の準同型であるときに f を同型写像といい、M_1 と M_2 は R 加群として同型であるという。

問題 5.5. R 加群準同型 $f : M_1 \to M_2$ が同型である必要十分条件は、全単射であることであることを示せ。

R 加群の準同型定理は次の通りである。

定理 5.1.7. M を左 R 加群とする。M 上の同値関係 $\sim$ が M に指定された全ての演算とコンパチブルである、すなわち

$$m_1 \sim m_2, m_1' \sim m_2' \Rightarrow m_1 + m_2 \sim m_1' + m_2', r \bullet m_1 \sim r \bullet m_2$$

であるとする。（単位元や単項演算についてはコンパチビリティは自動的に成立する、命題 2.4.19 の証明同様に示される。）

このとき、$[0]_\sim$ は M の左部分 R 加群となる。

逆に、M の左 R 部分加群 N に対し、

$$m_1 \sim m_2 \Leftrightarrow m_1 - m_2 \in N$$

なる二項関係 $\sim$ を定義するとこれは同値関係で、M に指定されたすべての演算とコンパチブルである。

系 5.1.8. M を左 R 加群、N をその左 R 部分加群とする。M/N には

$$q : M \to M/N$$

を R 加群準同型とするような加群の構造がただ一通りに入る。具体的には、

$$[m_1] + [m_2] := [m_1 + m_2], \quad r \bullet [m] := [r \bullet m]$$

となる。

系 5.1.9. $f : M \to M'$ を左 R 加群準同型とするとき、$\mathrm{Ker} f \subset M$ も左 R 加群、像 $f(M) \subset M'$ も左 R 加群であり、

$$M/\mathrm{Ker} f \to f(M)$$

なる同形が与えられる。

系 5.1.10. f が単射であることと、$\mathrm{Ker} f = 0$ とは同値。

証明は、群や環の準同型定理の証明と大差ない。

問題 5.6. 上の定理とその系を証明せよ。

5.2　直和と自由 R 加群

定義 5.2.1. R を環とし、M_1, M_2 を左 R 加群とする。M_1 と M_2 の直和 (direct sum)$M_1 \oplus M_2$ とは、

1. 加法群としては直積 $M_1 \times M_2$
2. R の作用はそれぞれに作用させる

ことで得られる左 R 加群である。書き下せば、

$$M_1 \oplus M_2 = \{(m_1, m_2) | m_1 \in M_1, m_2 \in M_2\}$$

$$(m_1, m_2) + (m_1', m_2') := (m_1 + m_1', m_2 + m_2'), \quad r \bullet (m_1, m_2) := (r \bullet m_1, r \bullet m_2)$$

で定まる左 R 加群のこと。

例 5.2.2. R を環とし、R^n を R の n 個の直積に、成分ごとの和と成分ごとの R の左作用

$$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n)$$

$$r \bullet (x_1, \ldots, x_n) = (r \cdot x_1, \ldots, r \cdot x_n)$$

を与えたものとする。これは左 R 加群である。直和の定義より

$$R^n = R \oplus R \oplus \cdots \oplus R \quad (n \text{ 個})$$

に他ならない。

左 R 加群 M であって、ある n により R^n と R 加群として同型なものを有限生成自由 R 加群という。

以下、$\bullet$ を省略する。

定義 5.2.3. R を環とする。左 R 加群 M に対し、M の（有限）基底 (basis) とはつぎのような性質を持つ M の元の列 $x_1, \ldots, x_n \in M$ である。

1. 一次独立性　$r_1 x_1 + \cdots + r_n x_n = 0 \quad \Rightarrow \quad r_1 = r_2 = \cdots = r_n = 0$
2. 生成　$< x_1, \ldots, x_n >_R := \{r_1 x_1 + \cdots + r_n x_n = 0 | r_i \in R\}$ は M に一致する。

2 番目の性質を、M は R 上 $x_1, \ldots, x_n$ で左 R 加群として生成されるという。このような $x_1, \ldots, x_n$ が存在するとき、M は左 R 加群として有限生成であるという。

定理 5.2.4. 左 R 加群 M が有限生成自由 R 加群である必要十分条件は、M が (有限) 基底を持つことである。

証明. 十分性：$f : R^n \to M$ を $(r_1, \ldots, r_n) \mapsto r_1 x_1 + \cdots + r_n x_n$ で与えれば R 加群準同型である。これが単射であるには系 5.1.10 により $\mathrm{Ker} f = \{0\}$ を言えばよいが、それが基底の条件の一次独立性に他ならない。f が全射であることは生成性に他ならない。

必要性:$\varphi : R^n \to M$ を R 加群の同型射とする。$(1, 0, 0, \ldots, 0), (0, 1, 0, \ldots, 0), \ldots, (0, \ldots, 0, 1)$ たちの φ による像を $x_1, \ldots, x_n$ とする。φ の単射性が一次独立性に他ならず、全射性が生成性に他ならない。 □

R が体、すなわち線形空間においては次のような強いことが言える。

定理 5.2.5. R が体のとき、有限生成 R 加群 V は基底を持つ。すなわち $V \cong R^n$。

これは、線形代数で習う「有限生成線形空間には基底が存在する」という定理に他ならない。
一般の環ではこのような性質は全く成り立たない。

$$\mathbb{Z}/n$$

は $\mathbb{Z}$ 加群であるが、自由 $\mathbb{Z}$ 加群ではない。
しかし、次のような性質が証明できる。このノートでは証明を与えない。

定理 5.2.6. （有限生成 PID 加群の構造定理）R が単項イデアル整域のとき、有限生成 R 加群 M は有限個の R と $R/(a)$ の形の加群の直和と (R 加群として) 同型である:

$$M \cong R^n \oplus R/(a_1) \oplus \cdots \oplus R/(a_s).$$

このような a_i は一意ではない。一意にするには次のようにする。

定理 5.2.7. 上の定理において、a_i を全て素元の冪乗にすることができる。その場合、$a_1, \ldots, a_{s-1}$ は可逆元倍と順序の入れ替えを除いて一意にさだまる。

M を加法群とする。$\mathrm{End}(M)$ は単位的環であるから、命題 4.2.6 により唯一つの単位的環準同型 ρ により

$$\rho : \mathbb{Z} \to \mathrm{End}(M)$$

となる。したがって、全ての加法群はただ一通りの方法によって（単位的）$\mathbb{Z}$ 加群となる。より具体的に書けば、$n \in \mathbb{Z}$ に対し $n \geq 0$ ならば

$$n \bullet m := m + m + \cdots + m \quad (n \text{ 個})$$

$n < 0$ ならば

$$n \bullet m := -(m + m + \cdots + m) \quad (-n \text{ 個})$$

で与えられる。

命題 5.2.8. 加法群は $\mathbb{Z}$ 加群であり、$\mathbb{Z}$ 加群は加法群である。$\mathbb{Z}$ 加群としての準同型と、加法群としての準同型は一致する。

問題 5.7. 上の命題を証明せよ。

$\mathbb{Z}$ は単項イデアル整域であったから、次を得る。

定理 5.2.9. (有限生成アーベル群の構造定理) M を有限生成加法群とすると、適当な $a_i \in \mathbb{Z}$ により

$$M = \mathbb{Z}^n \oplus \mathbb{Z}/(a_1) \oplus \cdots \oplus \mathbb{Z}/(a_s)$$

の形に書くことができる。a_i を全て素数冪と選ぶこともでき、その場合は a_i は順番の入れ替えをのぞきただ一通りに決まる。

特に、有限加法群は有限生成であるから、上の形にあらわされて $n = 0$ である。

問題 5.8. G を有限加法群とする。G の元の中で位数が最大なものをとり、その位数を G の指数 (exponent) といい $e(G)$ で表す。
任意の $g \in G$ に対し、$g^{e(G)} = e$ を示せ。

5.3　単因子論

定理 5.2.6 を用いると、Jordan 標準形の存在が容易に証明できる。
K を体とし、$A \in M_n(K)$ とする。定理 4.4.5 により、

$$\rho : K[t] \to \mathrm{End}_K(K^n), t \mapsto A$$

となる単位環準同型 ρ が一意に定まる。したがって、K^n は $K[t]$ 加群となる。具体的には

$$f(t) \bullet \mathbf{x} := f(A)\mathbf{x}$$

で $K[t]$ の作用が与えられる。
定理 5.2.6 により、K^n は

$$K^n \cong (K[t])^m \oplus K[t]/(a_1) \oplus \cdots \oplus K[t]/(a_s)$$

の形にかける。が、左辺は K 上有限次元なので $m = 0$ となる。$a_1, \ldots, a_s \in K[t]$ は素元（すなわち既約多項式）の冪であるとしてよい。$a_i = p_i^{m_i}$ であるとしよう。

定義 5.3.1. K を体とする。$K[t]$ の二次以上の多項式が全て既約でないとき、K を代数閉体という。

今、K を代数閉体とする。このとき、$p_i = t - \lambda_i$ である。$K[t]$ 加群の同型

$$K^n \cong K[t]/(a_1) \oplus \cdots \oplus K[t]/(a_s)$$

が与えられている。左辺へは t は A 倍として作用する。右辺へは t は t 倍として作用する。

$$0 \oplus 0 \oplus \cdots (t - a_i)^j \oplus 0 \oplus \cdots \oplus 0$$

$0 \leq j \leq m_i - 1$、の形のものを並べると基底となり、t 倍するという写像の表現行列は Jordan 標準形になる。よって、K^n に A が作用するのに、基底をとりなおせば表現行列を Jordan 標準形とすることができる。

参考文献

[1] 松坂和夫「集合・位相入門」岩波書店

[2] 松坂和夫「代数系入門」岩波書店

[3] N. Bourbaki, Elements of Mathematics:Algebra I, Chapters 1-3, Springer. ISBN: 978-3-540-64243-5

[4] S. Burris (著), H. P. Sankappanavar , A Course in Universal Algebra (Graduate Texts in Mathematics 78), 1981, Springer. ISBN: 978-0387905785

索 引