代数数理工学 第 0.04 版

@bd_gfngfn

2014 年 6 月 29 日

目次

0 はじめに

この文書は東京大学工学部で 2014 年度夏学期に開講されている代数数理工学の講義とそのノートをもとにしたものですが，作者の趣味により記号論理学的な形式的証明を多くの場面で用いています．題に「*」のついている章や節は，講義では特に扱われていない項目ではありますが理解の助けとして必要かと考えた内容を補ったものです．

1 *記号論理

1.1 *代数と記号論理

代数と形式的証明

命題を記号列，推論を記号列操作とみなして，その意味を無理に考えずとも証明できるようにした体系を**形式的証明**といいます[*1]．簡素な定義から様々な定理を導く代数は，形式的証明と非常に親和性の高い分野です．この文書では，しばしば見通しを良くするために一階述語論理による**自然演繹**で証明を記述しています[*2]．自然演繹は，各論理記号に対する**導入則**と**除去則**という推論からなる体系です．論理記号としては自然言語の「かつ」にあたる**連言** $\wedge$，「または」にあたる**選言** $\vee$，「ならば」にあたる**論理包含**或いは**含意** $\Rightarrow$，「でない」にあたる**否定** $\neg$，「任意の」にあたる**全称量化** $\forall$，「存在する」にあたる**存在量化** $\exists$ を基本とします．以下，一般の命題 $\Phi, \Psi, X \ldots$ に対して成り立つ推論規則を示します．

1.2 *命題論理

定義 1.2.1 古典論理，直観主義論理

自然演繹に於ける**古典論理**の体系 **NK** と**直観主義論理**の体系 **NJ** を掲げます．古典論理は $\wedge$，$\vee$，$\Rightarrow$，$\neg$ の導入則・除去則と**排中律**からなり，直観主義論理は $\wedge$，$\vee$，$\Rightarrow$，$\neg$ の導入則・除去則からなります．

定義 1.2.2 連言

連言 $\wedge$ の導入則 ($\wedge$-INTRO) と除去則 ($\wedge$-ELIM-L)，($\wedge$-ELIM-R) を以下のように定めます：

$$\frac{\Phi \qquad \Psi}{\Phi \wedge \Psi}\ (\wedge\text{-INTRO}) \qquad \frac{\Phi \wedge \Psi}{\Phi}\ (\wedge\text{-ELIM-L}) \qquad \frac{\Phi \wedge \Psi}{\Psi}\ (\wedge\text{-ELIM-R})$$

定義 1.2.3 選言

連言 $\wedge$ の導入則 ($\vee$-INTRO-L)，($\vee$-INTRO-R) と除去則 ($\vee$-ELIM) を以下のように定めます：

$$\frac{\Phi}{\Phi \vee \Psi}\ (\vee\text{-INTRO-L}) \qquad \frac{\Psi}{\Phi \vee \Psi}\ (\vee\text{-INTRO-R})$$

$$\dfrac{\Phi \vee \Psi \qquad \begin{array}{c}\Gamma \quad [\Phi]_1 \\ \vdots \\ X\end{array} \qquad \begin{array}{c}\Gamma \quad [\Psi]_1 \\ \vdots \\ X\end{array}}{X}\ (\vee\text{-ELIM})1$$

[*1] 20 世紀初頭，集合論が矛盾を孕んでいたことが発見されたのをきっかけとして論理学の記号化が発達し，形式的証明という様式が確立されました．意外に歴史の浅い分野です．

[*2] 東京大学教養学部前期課程で開講されている「記号論理学 I（理科生）」は多くの理科生が受講し，既にご存知の方も多いかと思いますが，念のためここに掲載しておきます．

定義 1.2.4 含意

含意 $\Rightarrow$ の導入則 ($\Rightarrow$-INTRO) と除去則 ($\Rightarrow$-ELIM) を以下のように定めます：

$$\dfrac{\dfrac{\Gamma \qquad [\Phi]_1}{\begin{array}{c}\vdots\\ \Psi\end{array}}}{\Phi \Rightarrow \Psi}\ (\Rightarrow\text{-INTRO})1 \qquad\qquad \dfrac{\Phi \qquad \Phi \Rightarrow \Psi}{\Psi}\ (\Rightarrow\text{-ELIM})$$

定義 1.2.5 否定

まず前提として，以下の**矛盾律**により矛盾 $\bot$ が導入されます：

$$\dfrac{\Phi \qquad \neg\Phi}{\bot}$$

この矛盾を用いて，否定 $\neg$ の導入則 ($\neg$-INTRO) および除去則 ($\neg$-ELIM) [*3]を以下のように定めます：

$$\dfrac{\dfrac{\Gamma \qquad [\Phi]_1}{\begin{array}{c}\vdots\\ \bot\end{array}}}{\neg\Phi}\ (\neg\text{-INTRO})\ 1 \qquad\qquad \dfrac{\bot}{\Phi}\ (\neg\text{-ELIM})\ 1$$

補足

実は，矛盾の記号 $\bot$ があれば否定の記号 $\neg$ がなくても論理体系の表現能力を損ないません．というのも，$\neg\Phi$ は $\Phi \Rightarrow \bot$ と同一視できるからです．

$$\dfrac{\Phi \qquad \Phi \Rightarrow \bot}{\bot}\ (\Rightarrow\text{-ELIM}) \qquad\qquad \dfrac{\dfrac{\Gamma \qquad [\Phi]_1}{\begin{array}{c}\vdots\\ \bot\end{array}}}{\Phi \Rightarrow \bot}\ (\Rightarrow\text{-INTRO})1$$

で矛盾律と否定の導入則を表現できます．しかしながら $\Phi \Rightarrow \bot$ よりも $\neg\Phi$ と表記した方が人間にとって見やすいので，表記上はこちらを採用します．

[*3] 除去則 ($\neg$-ELIM) は，**不条理則**と呼ばれることもあります．

定義 1.2.6 排中律

$$\frac{}{\Phi \vee \neg \Phi}$$

を**排中律**と呼びます．これは，どんな命題も成り立つか成り立たないかのどちらかである，という主張にあたります．古典論理ではこれを認め，直観主義論理ではこれを認めません．普通，数学では古典論理に根ざして推論することになっており，多くの人は知らないうちに自明視しているでしょう．例えば背理法[*4]の妥当性もこれに基づいています．実際の推論では，排中律と等価な

$$\frac{\neg\neg\Phi}{\Phi}$$

で表される**二重否定除去則**の方が扱いやすいことが多いかもしれません．

1.3 *述語論理

!!!!要加筆!!!!

[*4] 本当は背理法の定義によります．

2 写像，代数系

2.1 算法

定義 2.1.1 内算法，外算法

E を集合とし，A を $A \subseteq E \times E$ なる集合とします．写像 $\circ : A \to E$ を，A を定義域とする**内算法**と呼ぶことにします．特に $A = E \times E$ のとき，内算法 $\circ$ は E 上**全域で定義されている**といいます．また Ω を集合とし，写像 $\diamond : \Omega \times E \to E$ を，Ω を**作用域**とする**外算法**と呼びます．このようにして定められる内算法と外算法を，併せて**算法**と呼びます．以下，A の元 (a,b) が内算法 $\circ$ によって写される行き先を $a \circ b$ と書き表すことにします[*5]．

定義 2.1.2 代数系

集合 E 上にいくつかの算法 $\underset{1}{\circ}, \underset{2}{\circ}, \ldots, \underset{m}{\circ}$ および $\underset{1}{\diamond}, \underset{2}{\diamond}, \ldots, \underset{n}{\diamond}$ が定義されているとき，$(E, \underset{1}{\circ}, \underset{2}{\circ}, \ldots, \underset{m}{\circ}, \underset{1}{\diamond}, \underset{2}{\diamond}, \ldots, \underset{n}{\circ})$ を**代数系**あるいは**代数構造**と呼びます．

定義 2.1.3 全射，単射

$f : X \to Y$ とします．$\forall y \in Y, \exists x \in X\,(y = f(x))$ が成り立つとき，f は**全射**であるといいます．また，$\forall x_1 \forall x_2 \in X\,(f(x_1) = f(x_2) \Rightarrow x_1 = x_2)$ が成り立つとき，f は**単射**であるといいます．f が全射かつ単射であるとき，f は**全単射**であるといいます．

補足

単射は対偶をとって $\forall x_1 \forall x_2 \in X\,(x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2))$ とした方が直感的に把握しやすいでしょう．

[*5] このように，2 個を引数にとる写像を中央に配置して書く記法を**中置記法**といいます．普段慣れ親しんでいる加法 $+$ を $m+n$ のように書くのと同じです．ちなみに $f(x,y,\ldots)$ のように写像を引数より前に書くものは**ポーランド記法**，$(x,y,\ldots)f$ のように写像を引数より後に書くものは**逆ポーランド記法**と呼ばれます．

定義 2.1.4 像，逆像

X，Y を集合とします．写像 $f : X \to Y$ および $A \subseteq X$ なる集合 A に対して

$$f(A) := \{ y \in Y \mid \exists x \in A (f(x) = y) \}$$

で定義される集合 $f(A)$ を f による A の**像**と呼びます．感覚的に言えば，A の元が f で写される行き先全体が $f(A)$ ということです．また $B \subseteq Y$ なる集合 B に対して

$$f^{-1}(B) := \{ x \in X \mid f(x) \in B \}$$

で定義される集合 $f^{-1}(B)$ を f による B の**逆像**と呼びます．述語論理らしい記法で定めると，以下のようになります．

$$\overline{\forall A \in \mathfrak{P}X \, (y \in f(A) \Leftrightarrow (y \in Y \wedge \exists x \in A (y = f(x))))}$$

$$\overline{\forall B \in \mathfrak{P}Y \left(x \in f^{-1}(B) \Leftrightarrow (x \in X \wedge f(x) \in B) \right)}$$

補足

逆写像 $f^{-1} : Y \to X$ は f が全単射であるときしか定義できませんが，逆像は一般の写像について定義できます．$f(x) = y$ なる x が $x = a, b, \ldots$ と複数存在する場合は，逆像は $f^{-1}(\{y\}) = \{a, b, \ldots\}$ という具合です．あるいは $f(x) = y$ なる x が存在しない場合は $f^{-1}(\{y\}) = \varnothing$ です．ただし，$f(A) = B$ のとき $f^{-1}(B) = A$ とは限らないことに注意しなければなりません．

定理 2.1.5 *逆像と像の合成

$f : X \to Y$ なる写像 f，$B \subseteq Y$ なる集合 B に対して，$f\left(f^{-1}(B)\right) \subseteq B$.

証明　いま $y \in f\left(f^{-1}(B)\right)$ と仮定すると，$f\left(f^{-1}(B)\right)$ は $f^{-1}(B)$ の像なので $x \in f^{-1}(B)$ かつ $y = f(x)$ を満たす x が存在します．この x をとると，$x \in f^{-1}(B)$ と逆像の定義より $f(x) \in B$ であり，また $y = f(x)$ だったので，$y \in B$. よって $f\left(f^{-1}(B)\right) \subseteq B$. ■

定義 2.1.6 準同型，同型

$(E, \underset{E1}{\circ}, \ldots, \underset{Em}{\circ}, \underset{E1}{\diamond}, \ldots, \underset{En}{\diamond})$ と $(F, \underset{F1}{\circ}, \ldots, \underset{Fm}{\circ}, \underset{F1}{\diamond}, \ldots, \underset{Fn}{\diamond})$ を代数系とします．各 $j \in \{1, \ldots, n\}$ に対して $\underset{Ej}{\diamond}$ と $\underset{Fj}{\diamond}$ が同一の作用域 Ω_j を持ち，次の 2 条件を満たす写像 $f : E \to F$ が存在するとき，$(E, \ldots)$ と $(F, \ldots)$ は**準同型**であるといい，またそのような条件を満たす f を**準同型写像**と呼びます：

1. 各 $i \in \{1, \ldots, m\}$ に対する内算法 $\underset{Ei}{\circ}$ と $\underset{Fi}{\circ}$ および $E \times E$ の任意の元 (a, b) に対し，$a \underset{Ei}{\circ} b$ か $f(a) \underset{Fi}{\circ} f(b)$ の一方が定義されていれば他方も定義されており，$a \underset{Ei}{\circ} b = f(a) \underset{Fi}{\circ} f(b)$.
2. 各 $j \in \{1, \ldots, n\}$ に対する外算法 $\underset{Ej}{\diamond}$ と $\underset{Fj}{\diamond}$ および $\Omega_j \times E$ の任意の元 (ω, a) に対し，$f(\omega \underset{Ej}{\diamond} a) = \omega \underset{Fj}{\diamond} f(a)$.

特に準同型写像 f が全単射であるとき，この f を**同型写像**と呼び，$(E, \ldots)$ と $(F, \ldots)$ は**同型**であるといいます．

2.2 関係

定義 2.2.1 関係

E を集合とします．$R \subseteq E \times E$ なる R を E 上の**関係**と呼び，E の元 a，b に対して $(a,b) \in R$ であるとき，aRb と中置記法で述語に見せかけるように書きます．

補足

関係を述語のように見せて書くと確かに式の扱いの上で直感的に扱えますが，同時にこれの本来の姿が集合であるということを隠すブラックボックスにもなってしまいます．関係はもともと集合である，ということを忘れず気にとめておかねばならないでしょう．

定義 2.2.2 同値関係

集合 E 上の関係 $\sim$ が次の性質をいずれも満たすとき，$\sim$ を E 上の**同値関係**と呼びます：

$$\forall a \in E\,(a \sim a) \qquad \text{反射律} \tag{1}$$
$$\forall a \forall b \in E\,(a \sim b \Rightarrow b \sim a) \qquad \text{対称律} \tag{2}$$
$$\forall a \forall b \forall c \in E\,((a \sim b \wedge b \sim c) \Rightarrow a \sim c) \qquad \text{推移律} \tag{3}$$

定義 2.2.3 同値類

関係 $\sim$ を集合 E の中の同値関係とします．E の元 a，b に対して $a \sim b$ が成り立つとき，a と b は**同値**であるといいます．a と同値な E の元全体の集合を a の**同値類**と呼び，$\underset{\sim}{\langle a \rangle}$ と表すことにします．すなわち

$$\underset{\sim}{\langle a \rangle} := \{\, x \in E \mid x \sim a \,\} \tag{4}$$

です．感覚的に明らかなので証明は省略しますが，同値類には次のような性質があります：

$$\forall a \in E\,(a \in \underset{\sim}{\langle a \rangle}) \tag{5}$$
$$\forall a \forall b \in E\,(b \in \underset{\sim}{\langle a \rangle} \Rightarrow \underset{\sim}{\langle a \rangle} = \underset{\sim}{\langle b \rangle}) \tag{6}$$
$$\forall a \forall b \in E\,(a \sim b \Rightarrow \underset{\sim}{\langle a \rangle} = \underset{\sim}{\langle b \rangle}) \tag{7}$$
$$\forall a \forall b \in E\,(\neg(a \sim b) \Rightarrow \underset{\sim}{\langle a \rangle} \cap \underset{\sim}{\langle b \rangle} = \varnothing) \tag{8}$$

定義 2.2.4 商集合

関係 $\sim$ を E の中の同値関係とします．E の $\sim$ に関する同値類全体の集合を E の $\sim$ に関する**商集合**と呼び，$E/\sim$ と表すことにします．すなわち

$$E/\sim = \{\, \underset{\sim}{\langle x \rangle} \in \mathfrak{P}E \mid x \in E \,\} \tag{9}$$

です．例えば $E = \{a,b,\ldots\}$ に対しては $E/\sim = \{\underset{\sim}{\langle a \rangle}, \underset{\sim}{\langle b \rangle}, \ldots\}$ となります．

定義 2.2.5 内算法と同値関係の両立

E を集合とし，E の中の同値関係 $\sim$ と，E に対し全域で定義された内算法 $\circ$ が与えられていて，

$$\forall x_1 \forall x_2 \forall y_1 \forall y_2 \in E\,((x_1 \sim x_2 \wedge y_1 \sim y_2) \Rightarrow x_1 \circ y_1 \sim x_2 \circ y_2) \tag{10}$$

が成り立つとき，内算法 $\circ$ と 同値関係 $\sim$ は**両立**するといいます．

定義 2.2.6 外算法と同値関係の両立

E を集合とし，E の中の同値関係 $\sim$ と，Ω を作用域に持つ E の外算法 $\diamond$ が与えられていて，

$$\forall x_1 \forall x_2 \in E, \forall d \in \Omega \, (x_1 \sim x_2 \Rightarrow d \diamond x_1 \sim d \diamond x_2) \tag{11}$$

が成り立つとき，$\sim$ と $\diamond$ は両立するといいます．

補足

$\circ$ と $\sim$ が両立するとどんな恩恵があるかというと，x の同値類 $\langle x \rangle_{\sim}$ と y の同値類 $\langle y \rangle_{\sim}$ に $x \circ y$ の同値類 $\langle x \circ y \rangle_{\sim}$ を対応させる算法 $\overline{\circ} : E/\sim \times E/\sim \to E/\sim$ が，$E/\sim$ 上の内算法となるわけです．

定義 2.2.7 商構造

代数系 $(E, \underset{1}{\circ}, \underset{2}{\circ}, \ldots)$ のすべての算法が E 上の同値関係 $\sim$ と両立するとき，これらの算法の商によって商集合 $E/\sim$ の上に定められている代数系を $\sim$ による E の**商構造**と呼びます．

定理 2.2.8

$f : E \to F$ を代数系 $(E, \underset{E}{\circ}, \ldots)$ から代数系 $(F, \underset{F}{\circ}, \ldots)$ への準同型写像とし，さらにすべての算法は各々の代数系の全域で定義されているとします．このとき

$$\forall x \forall y \in E \, (x \sim y \Leftrightarrow f(x) = f(y)) \tag{12}$$

で関係 $\sim$ を定めると，これは E 上の同値関係となり，$\sim$ と $(E, \underset{E}{\circ}, \ldots)$ のすべての算法は両立します．

証明　$\sim$ の同値関係性は，一般の写像および等号の性質

$$\forall x \in E \, (f(x) = f(x))$$
$$\forall x \forall y \in E \, (f(x) = f(y) \Rightarrow f(y) = f(x))$$
$$\forall x \forall y \forall z \in E \, ((f(x) = f(y) \wedge f(y) = f(z)) \Rightarrow f(x) = f(z))$$

より明らかに成り立ちます．この同値関係 $\sim$ を f によって**生成される同値関係**といいます．f は準同型写像なので，$\underset{E}{\circ}$ および $\underset{F}{\circ}$ に対して

$$\forall x \forall y \in E \, (f(x \underset{E}{\circ} y) = f(x) \underset{F}{\circ} f(y))$$

が成り立ちます．いま $x_1 \sim x_2$，$y_1 \sim y_2$ を仮定すると，それぞれ $\sim$ の定義より $f(x_1) = f(x_2)$，$f(y_1) = f(y_2)$ であり，したがって

$$f(x_1 \underset{E}{\circ} y_1) = f(x_1) \underset{F}{\circ} f(y_1) = f(x_2) \underset{F}{\circ} f(y_2) = f(x_2 \underset{E}{\circ} y_2)$$

すなわち $x_1 \underset{E}{\circ} y_1 = x_2 \underset{E}{\circ} y_2$ が成り立ちます．$x_1, x_2, y_1, y_2 \in E$ は任意にとったので，題意は示されたことになります．■

定理 2.2.9 準同型定理

$(E, \underset{E}{\circ}, \ldots)$，$(F, \underset{F}{\circ}, \ldots)$ を代数系とし，$(E, \underset{E}{\circ}, \ldots)$ に於いてはすべての算法が全域で定義されているとします．このとき，$(E, \underset{E}{\circ}, \ldots)$ から $(F, \underset{F}{\circ}, \ldots)$ への準同型写像 f によって生成される同値関係 $\sim$ による E の商集合 $E/\sim$ は，f による E の像 $f(E) := \{ f(a) \mid a \in E \} = \{ y \in F \mid \exists x \in F \, (y = f(x)) \}$ と同型．

証明　まず $\sim$ の定義より $\forall x\forall y\in E\,(x\sim y\Rightarrow f(x)=f(y))$ なので $\forall a\in E,\forall x\forall y\in\underset{\sim}{\langle a\rangle}\,(f(x)=f(y))$ であり

$$\begin{array}{rccc}\mathscr{F}: & E/\sim & \longrightarrow & f(E)\\ & \cup & & \cup\\ & \underset{\sim}{\langle a\rangle} & \longmapsto & f(a)\end{array}$$

なる写像 $\mathscr{F}$ が定義できます．この $\mathscr{F}$ は

$$\begin{aligned}\mathscr{F}(\underset{\sim}{\langle a\rangle})=\mathscr{F}(\underset{\sim}{\langle b\rangle}) &\iff f(a)=f(b)\\ &\iff a\sim b && (f\text{ の定義より})\\ &\iff \underset{\sim}{\langle a\rangle}=\underset{\sim}{\langle b\rangle}\end{aligned}$$

より単射であり，また

$$\begin{aligned}b\in f(E) &\iff \exists a\in E\,(b=f(a))\\ &\iff \exists a\in E\,(b=\mathscr{F}(\underset{\sim}{\langle a\rangle}))\\ &\iff \exists A\in E/\sim\,(b=\mathscr{F}(A))\end{aligned}$$

より全射．よって $\mathscr{F}:E/\sim\to f(E)$ は同型写像であり，$E/\sim$ と $f(E)$ は同型となっています．　■

2.3 可逆化

定義 2.3.1

集合 E とその上の内算法 $\circ$，および $A,B\subseteq E$ なる A，B に対して $A\circ B:=\{a\circ b\in E\,|\,a\in A\wedge b\in B\}$ で $A\circ B$ を定めます．また，$\{a\}\circ B$ は $a\circ B$，$A\circ\{b\}$ は $A\circ b$ とそれぞれ略記することとします．

定義 2.3.2 安定集合

$A\subseteq E$ なる A が $A\circ A\subseteq A$ を満たすとき，A は算法 $\circ$ に関して**安定**であるとか**安定集合**であるといいます．また，$S\subseteq E$ なる S に対して $S\subseteq A$ かつ $A\subseteq E$ を満たす最小の安定集合 A を S から**生成される安定集合**といいます．

例

非負整数 $\mathbf{N}$ とその上の加法 $+$ からなる代数系 $(\mathbf{N},+)$ に於いて，偶数全体の集合は $+$ に関して安定．

定義 2.3.3 正則元

代数系 $(E,\circ)$ に於いて，$a\in E$ とし，$x\in E$ なる x を $a\circ x$ に写す写像および $x\circ a$ に写す写像がともに単射であるとき，a を算法 $\circ$ に関する**正則元**と呼びます．

例

$(\mathbf{N},+)$ に於いて $a\in\mathbf{N}$ は $n\mapsto a+n$ および $n\mapsto n+a$ がいずれも単射なので，$a\in\mathbf{N}$ なる任意の a は正則元．

定理 2.3.4 可逆化

内算法 $\circ$ は集合 E 上全域で定義され，結合的かつ可換であるとします．$(E,\circ)$ の正則元全体からなる集合を E^* とし，関係 $\sim$ を

$$\forall(x_1,y_1)\forall(x_2,y_2)\in E\times E^*\left((x_1,y_1)\sim(x_2,y_2)\Leftrightarrow x_1\circ y_2=x_2\circ y_1\right)$$

で定めると，$\sim$ は $E\times E^*$ 上の同値関係となります．ここで $E\times E^*$ 上の内算法 $\overline{\circ}$ を

$$(x,y)\overline{\circ}(p,q):=(x\circ p,y\circ q)$$

で定めると，$\overline{\circ}$ と $\sim$ は両立します．すなわち

$$\begin{aligned}&\forall(x_1,y_1)\forall(x_2,y_2)\forall(p_1,q_1)\forall(p_2,q_2)\in E\times E^*\\&\quad\left(((x_1,y_1)\sim(x_2,y_2)\wedge(p_1,q_1)\sim(p_2,q_2))\Rightarrow(x_1,y_1)\overline{\circ}(p_1,q_1)\sim(x_2,y_2)\overline{\circ}(p_2,q_2)\right)\end{aligned}$$

が成り立ちます．このとき $\overline{E}:=(E\times E^*)/_\sim$ とすると，

$$\underset{\sim}{\langle(x,y)\rangle}\,\overline{\circ}\,\underset{\sim}{\langle(p,q)\rangle}:=\underset{\sim}{\left\langle(x,y)\overline{\circ}(p,q)\right\rangle}$$

によって $\overline{E}$ 上の内算法 $\overline{\circ}$ が定められます．このとき，$\overline{\circ}$ に関して安定な $\overline{E}$ の部分集合 A を，以下の条件を満たすように決めることができます：

1. $(E,\circ)$ から $(A,\overline{\circ})$ への同型写像 f が存在する．
2. $\forall a\in E^*\left(f(a)\in A\wedge(f(a))^{-1}\in\overline{E}\right)$．
3. $\overline{E}$ は A と A の正則元の逆元全体との和集合から生成される．

補足

一見複雑な処理をしていますが，結局可逆化とはどんな処理なのかというと，結合律と交換律を満たすもとの代数系 $(E,\circ)$ をうまく“拡張”して，単位元を含み任意の元が逆元を持つ代数系 $\left(\overline{E},\overline{\circ}\right)$ をつくれるということです．より感覚的に“逆元で閉じるように拡張する”と言ってもよいでしょう．このような，結合律と交換律を満たし，単位元と各元に対する逆元を持つ代数系は**可換群**と呼ばれ，この文書でも後述します．例は直後に挙げますが，例えば自然数[*6]$\mathbf{N}$ の元は $+$ について $\mathbf{N}$ 内に逆元を持ちません（すなわち $n\in\mathbf{N}$ に対して $n+\overline{n}=0$ を満たす $\overline{n}\in\mathbf{N}$ は存在しません）が，これを逆元で閉じるように“拡張”すると $(\mathbf{Z},+)$ となり，加法 $+$ に関して可換群となるのです[*7]．

[*6] ここでは非負整数のことを指します．

[*7] $(\mathbf{N},+)$ の加法 $+$ と $(\mathbf{Z},+)$ の加法 $+$ は，結果的に同じ感覚で扱えますが本来は別の演算であるということに注意しましょう．直後の例では明示的に $\underset{\mathbf{N}}{+}$ と $\underset{\mathbf{Z}}{+}$ で両者を区別したので確認してください．

例

$(\mathbf{N},\underset{\mathbf{N}}{+})$ から $(\mathbf{Z},\underset{\mathbf{Z}}{+})$ への可逆化：　$E:=\mathbf{N}$，$E^*:=\mathbf{N}$ として，

$$\forall(x_1,y_1)\forall(x_2,y_2)\in\mathbf{N}\times\mathbf{N}\,((x_1,y_1)\sim(x_2,y_2)\Leftrightarrow x_1\underset{\mathbf{N}}{+}y_2=x_2\underset{\mathbf{N}}{+}y_1)$$

で $\mathbf{N}\times\mathbf{N}$ 上の同値関係 $\sim$ を定めます．これは，感覚的には $x_1-y_1=x_2-y_2$ のように減法で表現したいところを加法 $\underset{\mathbf{N}}{+}$ で表しているのです．$E\times E^*=\mathbf{N}\times\mathbf{N}$ 上の加法 $\underset{\mathbf{N}\times\mathbf{N}}{+}$ を

$$(x_1,y_1)\underset{\mathbf{N}\times\mathbf{N}}{+}(x_2,y_2):=(x_1\underset{\mathbf{N}}{+}x_2,y_1\underset{\mathbf{N}}{+}y_2)$$

で定め，さらに $\mathbf{Z}:=\overline{E}=(E\times E^*)/_\sim=(\mathbf{N}\times\mathbf{N})/_\sim$ で定義される $\mathbf{Z}$ 上の加法 $\underset{\mathbf{Z}}{+}$ を

$$\langle(x_1,y_1)\rangle_\sim\underset{\mathbf{Z}}{+}\langle(x_2,y_2)\rangle_\sim:=\langle(x_1,y_1)\underset{\mathbf{N}\times\mathbf{N}}{+}(x_2,y_2)\rangle_\sim$$

で定義すると，$\langle(w,w)\rangle_\sim$ が $\mathbf{Z}$ の $\underset{\mathbf{Z}}{+}$ に関する単位元となり，また $\langle(x\underset{\mathbf{N}}{+}y,y)\rangle_\sim$ の逆元は $\langle(y,x\underset{\mathbf{N}}{+}y)\rangle_\sim$ となります．

例

$(\mathbf{Z},\underset{\mathbf{Z}}{\bullet})$ から $(\mathbf{Q},\underset{\mathbf{Q}}{\bullet})$ への可逆化：　$E:=\mathbf{Z}$，$E^*:=\mathbf{Z}^*:=\mathbf{Z}\backslash\{0\}$ として，やはり

$$\forall(x_1,y_1)\forall(x_2,y_2)\in\mathbf{Z}\times\mathbf{Z}^*\,((x_1,y_1)\sim(x_2,y_2)\Leftrightarrow x_1\underset{\mathbf{Z}}{\bullet}y_2=x_2\underset{\mathbf{Z}}{\bullet}y_1)$$

で $\mathbf{Z}\times\mathbf{Z}^*$ 上の同値関係 $\sim$ を定めます．$\mathbf{Z}\times\mathbf{Z}^*$ 上の乗法 $\underset{\mathbf{Z}\times\mathbf{Z}^*}{\bullet}$ を

$$(x_1,y_1)\underset{\mathbf{Z}\times\mathbf{Z}^*}{\bullet}(x_2,y_2):=(x_1\underset{\mathbf{Z}}{\bullet}x_2,y_1\underset{\mathbf{Z}}{\bullet}y_2)$$

で定め，さらに $\mathbf{Q}:=(\mathbf{Z}\times\mathbf{Z}^*)/_\sim$ で定義される $\mathbf{Q}$ 上の乗法 $\underset{\mathbf{Q}}{\bullet}$ を

$$\langle(x_1,y_1)\rangle_\sim\underset{\mathbf{Q}}{\bullet}\langle(x_2,y_2)\rangle_\sim:=\langle(x_1,y_1)\underset{\mathbf{Z}\times\mathbf{Z}^*}{\bullet}(x_2,y_2)\rangle_\sim$$

で定義すると，$\langle(w,w)\rangle_\sim$ が $\mathbf{Q}$ の $\underset{\mathbf{Q}}{\bullet}$ に関する単位元となり，また $\langle(x\underset{\mathbf{Z}}{\bullet}y,y)\rangle_\sim$ の逆元は $\langle(y,x\underset{\mathbf{Z}}{\bullet}y)\rangle_\sim$ となります．

補足

主に数学基礎論で取り扱われる題材ですが，我々が普段一応直感的に用いている自然数 $\mathbf{N}$，整数 $\mathbf{Z}$，有理数 $\mathbf{Q}$，実数 $\mathbf{R}$ は，

$$\cdots\xrightarrow{\text{公理的集合論}}\mathbf{N}\xrightarrow{\text{加法}+\text{の可逆化}}\mathbf{Z}\xrightarrow{\text{乗法}\bullet\text{の可逆化}}\mathbf{Q}\xrightarrow{\text{差の絶対値を距離とする完備化}}\mathbf{R}$$

という“拡張”の過程を経て，演繹的推論による妥当性を以て構成することができます．

3 束論

3.1 束，半順序関係

定義 3.1.1 束

L を集合とし，L 上全域で定義された 2 つの内算法 $\vee$ と $\wedge$ が

$\forall a\forall b\forall c \in L((a\vee b)\vee c = a\vee(b\vee c))$	$\vee$ の結合律
$\forall a\forall b\forall c \in L((a\wedge b)\wedge c = a\wedge(b\wedge c))$	$\wedge$ の結合律
$\forall a\forall b \in L(a\vee b = b\vee a)$	$\vee$ の交換律
$\forall a\forall b \in L(a\wedge b = b\wedge a)$	$\wedge$ の交換律
$\forall a\forall b \in L((a\wedge b)\vee a = a)$	吸収律
$\forall a\forall b \in L((a\vee b)\wedge a = a)$	吸収律

を満たすとき，この代数系 $(L,\vee,\wedge)$ を束と呼びます[*8]．L の元 a，b に対し $a\vee b$ を a と b の上限，$a\wedge b$ を a と b の下限と呼ぶことにします[*9]．

例

A を集合とし，$X,Y\subseteq A$ なる X，Y に対して $X\cup Y$ を和集合，$X\cap Y$ を積集合とすると，代数系 $(\mathfrak{P}A,\cup,\cap)$ は束．

定義 3.1.2 *束に関する証明木の記法

証明木を書くにあたり，述語論理の純粋な自然演繹ではきわめて煩雑となるので，束 L の元 a，b，c に関する結合律 (Assoc)，交換律 (Commu)，吸収律 (Absorb) をそれぞれ

$$\frac{}{(a\vee b)\vee c = a\vee(b\vee c)}\ (\textsc{Assoc}) \qquad \frac{}{a\vee b = b\vee a}\ (\textsc{Commu}) \qquad \frac{}{(a\wedge b)\vee a = a}\ (\textsc{Absorb})$$

$$\frac{}{(a\wedge b)\wedge c = a\wedge(b\wedge c)}\ (\textsc{Assoc}) \qquad \frac{}{a\wedge b = b\wedge a}\ (\textsc{Commu}) \qquad \frac{}{(a\vee b)\wedge a = a}\ (\textsc{Absorb})$$

という具合に書くこととします．

定理 3.1.3 *束の冪等律

$(L,\vee,\wedge)$ を束とすると，L の元 x について $x\vee x = x$，$x\wedge x = x$ が成り立ちます．

[*8] 演算を省略して単に集合 L を束と呼ぶこともありますが，ここではできるだけ省略せず書くこととします．

[*9] $a\vee b$ を結び，$a\wedge b$ を交わりと呼ぶこともあります．

証明

$$\dfrac{\dfrac{\dfrac{}{(x\vee y)\wedge x = x\wedge(x\vee y)}\,(\text{Commu})\quad \dfrac{}{(x\vee y)\wedge x = x}\,(\text{Absorb})}{x\wedge(x\vee y) = x}\qquad \dfrac{}{(x\wedge(x\vee y))\vee x = x}\,(\text{Absorb})}{x\vee x = x}$$

$$\dfrac{\dfrac{\dfrac{}{(x\wedge y)\vee x = x\vee(x\wedge y)}\,(\text{Commu})\quad \dfrac{}{(x\wedge y)\vee x = x}\,(\text{Absorb})}{x\vee(x\wedge y) = x}\qquad \dfrac{}{(x\vee(x\wedge y))\wedge x = x}\,(\text{Absorb})}{x\wedge x = x}$$

■

以降では冪等律を以下のように書くこととします．

$$\dfrac{}{x\vee x = x}\,(\text{Idem})\qquad\qquad \dfrac{}{x\wedge x = x}\,(\text{Idem})$$

定義 3.1.4 半順序関係

集合 P 上の関係 $\preccurlyeq$ が

$\forall x\in P\,(x\preccurlyeq x)$	反射律
$\forall x\forall y\in P\,((x\preccurlyeq y\wedge y\preccurlyeq x)\Rightarrow x=y)$	反対称律
$\forall x\forall y\forall z\in P\,((x\preccurlyeq y\wedge y\preccurlyeq z)\Rightarrow x\preccurlyeq z)$	推移律

を満たすとき，$\preccurlyeq$ を P 上の**半順序関係**と呼びます．また $(P,\preccurlyeq)$ を**半順序集合**と呼びます．

補足

E の元 x，y に対して $x\preccurlyeq y$ または $y\preccurlyeq x$ が成り立つとき，x と y が**比較可能**であるといいます．E の任意の 2 元が比較可能であるとき，$\preccurlyeq$ を**全順序**あるいは**線型順序**と呼びます．全順序は通常の $\mathbf{N}$ 上の不等号 $\leq$ と同様に序列を形成します．

定義 3.1.5 *半順序関係に関する証明木の記法

半順序集合 P の元 a，b に対して，述語論理による純粋な自然演繹では

$$\dfrac{a \in P \qquad \dfrac{\dfrac{}{\forall x \in P\,(x \preccurlyeq x)}\,(\textsc{Ref})}{a \in P \Rightarrow a \preccurlyeq a}}{a \preccurlyeq a}$$

$$\dfrac{\dfrac{a \preccurlyeq b \qquad b \preccurlyeq a}{a \preccurlyeq b \wedge b \preccurlyeq a} \qquad \dfrac{b \in P \qquad \dfrac{\dfrac{\dfrac{\dfrac{}{\forall x \forall y \in P\,((x \preccurlyeq y \wedge y \preccurlyeq x) \Rightarrow x = y)}\,(\textsc{AntiSym})}{a \in P \qquad a \in P \Rightarrow \forall y \in P\,(a \preccurlyeq y \wedge y \preccurlyeq a) \Rightarrow a = y}}{\forall y \in P\,(a \preccurlyeq y \wedge y \preccurlyeq a) \Rightarrow a = y}}{b \in P \Rightarrow (a \preccurlyeq b \wedge b \preccurlyeq a) \Rightarrow a = b}}{(a \preccurlyeq b \wedge b \preccurlyeq a) \Rightarrow a = b}}{a = b}$$

$$\dfrac{\dfrac{a \preccurlyeq b \qquad b \preccurlyeq c}{a \preccurlyeq b \wedge b \preccurlyeq c} \qquad \dfrac{c \in P \qquad \dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\forall x \forall y \forall z \in P\,((x \preccurlyeq y \wedge y \preccurlyeq z) \Rightarrow x \preccurlyeq z)}\,(\textsc{Trans})}{a \in P \qquad a \in P \Rightarrow \forall y \forall z \in P\,(a \preccurlyeq y \wedge y \preccurlyeq z) \Rightarrow a \preccurlyeq z}}{\forall y \forall z \in P\,(a \preccurlyeq y \wedge y \preccurlyeq z) \Rightarrow a \preccurlyeq z}}{b \in P \qquad b \in P \Rightarrow \forall z \in P\,(a \preccurlyeq b \wedge b \preccurlyeq z) \Rightarrow a \preccurlyeq z}}{\forall z \in P\,(a \preccurlyeq b \wedge b \preccurlyeq z) \Rightarrow a \preccurlyeq z}}{c \in P \qquad c \Rightarrow (a \preccurlyeq b \wedge b \preccurlyeq c) \Rightarrow a \preccurlyeq c}}{(a \preccurlyeq b \wedge b \preccurlyeq c) \Rightarrow a \preccurlyeq c}}{a \preccurlyeq c}$$

という具合に反射律 (Ref)，反対称律 (AntiSym)，推移律 (Trans) による推論がそれぞれ書けますが，これではあまりにも煩雑なので，全称量化と $a,b,c \in P$ の仮定を省略してそれぞれ

$$\dfrac{}{a \preccurlyeq a}\,(\textsc{Ref}) \qquad \dfrac{a \preccurlyeq b \qquad b \preccurlyeq a}{a = b}\,(\textsc{AntiSym}) \qquad \dfrac{a \preccurlyeq b \qquad b \preccurlyeq c}{a \preccurlyeq c}\,(\textsc{Trans})$$

と簡潔に記すことにします．

定理 3.1.6 束からの半順序関係の構成

代数系 $(L,\vee,\wedge)$ を束とします．このとき

$$\forall a \forall b \in L\,(a = a \wedge b \Leftrightarrow a \preccurlyeq b)$$

で定められる関係 $\preccurlyeq$ は半順序関係となります．

証明　$\preccurlyeq$ が反射律，反対称律，推移律を満たすことを示します．まず

$$\dfrac{\dfrac{}{a \wedge a = a}\,(\textsc{Idem})}{a \preccurlyeq a}\,(\preccurlyeq)$$

より，反射律が成り立ちます．また

$$\dfrac{\dfrac{\dfrac{[a \preccurlyeq b \wedge b \preccurlyeq a]_1}{\dfrac{a \preccurlyeq b}{a = a \wedge b}\,(\preccurlyeq)} \qquad \dfrac{\dfrac{[a \preccurlyeq b \wedge b \preccurlyeq a]_1}{\dfrac{b \preccurlyeq a}{b = b \wedge a}\,(\preccurlyeq)} \qquad \dfrac{}{a \wedge b = b \wedge a}\,(\textsc{Commu})}{b = a \wedge b}}{a = b}\,1}{(a \preccurlyeq b \wedge b \preccurlyeq a) \Rightarrow a = b}$$

より，反対称律が成り立ちます．さらに

$$\dfrac{\dfrac{\dfrac{\dfrac{[a \preccurlyeq b \wedge b \preccurlyeq c]_2}{\dfrac{a \preccurlyeq b}{a = a \wedge b}\,(\preccurlyeq)} \qquad \dfrac{\dfrac{[a \preccurlyeq b \wedge b \preccurlyeq c]_2}{\dfrac{a \preccurlyeq b}{a = a \wedge b}\,(\preccurlyeq)} \qquad \dfrac{\dfrac{[a \preccurlyeq b \wedge b \preccurlyeq c]_2}{\dfrac{b \preccurlyeq c}{b = b \wedge c}\,(\preccurlyeq)}}{a = a \wedge (b \wedge c)} \qquad \dfrac{}{(a \wedge b) \wedge c = a \wedge (b \wedge c)}\,(\textsc{Assoc})}{a = (a \wedge b) \wedge c}}{\dfrac{a = a \wedge c}{a \preccurlyeq c}\,(\preccurlyeq)}}{(a \preccurlyeq b \wedge b \preccurlyeq c) \Rightarrow a \preccurlyeq c}\,2$$

より，推移律が成り立ちます．以上より，$\preccurlyeq$ は L 上の半順序関係となっています． ■

定義 3.1.7 モジュラ束

束 $(L, \vee, \wedge)$ および定理 3.1.6 により定められる半順序関係 $\preccurlyeq$ が

$$\forall x \forall z \in L\,(x \preccurlyeq z \Rightarrow \forall y \in L\,((x \vee y) \wedge z = x \vee (y \wedge z)))$$

を満たすとき，$(L, \vee, \wedge)$ を**モジュラ束**と呼びます．

定義 3.1.8 分配束

束 $(L, \vee, \wedge)$ が

$$\forall x \forall y \forall z \in L\,((x \wedge z) \vee (y \wedge z) \preccurlyeq (x \vee y) \wedge z) \qquad \forall x \forall y \forall z \in L\,((x \vee z) \wedge (y \vee z) \preccurlyeq (x \wedge y) \vee z)$$

をいずれも満たすとき，$(L, \vee, \wedge)$ を**分配束**と呼びます．

!!!!要加筆!!!!

4 群論

4.1 群の基本

定義 4.1.1 群，可換，可換群，非可換群，有限群

G を集合とします． G 上全域で定義された内算法 $\cdot$ が

$$\forall x\forall y\forall z\in G\left((x\cdot y)\cdot z=x\cdot(y\cdot z)\right) \qquad \text{結合律} \tag{13}$$

$$\exists e\forall x\in G\left(e\cdot x=x\wedge x\cdot e=x\wedge\exists y(x\cdot y=e\wedge y\cdot x=e)\right) \qquad \text{単位元の存在と逆元の存在} \tag{14}$$

を満たすとき，$(G,\cdot)$ を**群**と呼びます[*10]．(14) 式のような e を $(G,\cdot)$ の**単位元**と呼びます．また同 (14) 式のような y を x の**逆元**と呼びます．特に $(G,\cdot)$ が

$$\forall a\forall b\in G(a\cdot b=b\cdot a) \qquad \text{交換律}$$

を満たすとき，内算法 $\cdot$ は**可換**であるといい，$(G,\cdot)$ を**可換群**と呼びます．また，交換律を満たさないときは $(G,\cdot)$ を**非可換群**と呼びます．さらに，G が有限集合であるとき，$(G,\cdot)$ を**有限群**と呼びます．

補足

慣習として，内算法を $\cdot$ と書く群は，この内算法を乗法と呼んで単位元を e や 1 で，x の逆元を x^{-1} で書き表すことが一般的です．また同様に内算法を $+$ と書く群は，この内算法を加法と呼んで単位元を 0 で，x の逆元を $-x$ で書き表すことが一般的です．普通，$+$ は可換な内算法を表すのに使われます．

定理 4.1.2

代数系 $(G,\cdot)$ が群ならば $G\neq\varnothing$.

証明　$G=\varnothing$ と仮定すると単位元が存在せず矛盾． ■

定理 4.1.3 単位元の一意的存在

群 $(G,\cdot)$ の単位元は一意的に存在します．

証明

いま e_1，e_2 がともに $(G,\cdot)$ の単位元であると仮定すると，単位元の定義より任意の G の元 x に対して $e_1\cdot x=x$，$x\cdot e_2=x$ が成り立つから，

$$e_1=e_1\cdot e_2=e_2$$

より $e_1=e_2$ となります． ■

[*10] 内算法 $\cdot$ が文脈上明らかなときは，省略して単に G を群と呼ぶこともあります．

補足

定義上，単位元は単に「～な性質を満たす G の元 e が存在する」とだけ定められていましたが，その性質により一意的にしか存在しえないことがわかるわけです．したがって或る代数系 $(G,\cdot)$ が群をなすことが判ったとき，その単位元 e は自然に定まるので，定数のように扱うことができます．

4.2 部分群

定義 4.2.1 部分群

群 $(G,\cdot)$ と $H\subseteq G$ なる H に対し，$(H,\cdot)$ が群をなすとき，この $(H,\cdot)$ は $(G,\cdot)$ の**部分群**であるといいます．内算法 $\cdot$ が文脈から明らかなときは，これを $H\leq G$ と書き表します．

定理 4.2.2

群 $(G,\cdot)$ と $H\subseteq G$ なる H に対し，

$$(H,\cdot)\text{ が }(G,\cdot)\text{ の部分群である}\Leftrightarrow\forall x\forall y\in H\left(x^{-1}\cdot y\in H\right)$$

が成り立ちます．

定理 4.2.3 部分群による同値関係

群 $(H,\cdot)$ が 群 $(G,\cdot)$ の部分群であるとき，

$$\forall x\forall y\in G\left(x\sim y\Leftrightarrow x^{-1}\cdot y\in H\right)$$

で関係 $\sim$ を定めると，この $\sim$ は同値関係となります．

証明　$x\in G$ に対し $x^{-1}\cdot x=e\in H$ より反射律が，$x,y\in G$ に対し $x^{-1}\cdot y\in H$ ならば $y^{-1}\cdot x=\left(x^{-1}\cdot y\right)^{-1}\in H$ より対称律が，$x,y,z\in G$ に対し $x^{-1}\cdot y$ かつ $y^{-1}\cdot z$ ならば $x^{-1}\cdot z=\left(x^{-1}\cdot y\right)\cdot\left(y^{-1}\cdot z\right)\in H$ より推移律がそれぞれ成り立ちます．■

定義 4.2.4 算法による集合の記法

群 $(G,\cdot)$ と G の元 a，$K,L\subseteq G$ なる K，L に対して，

$$\begin{aligned}a\cdot K&:=\{a\cdot k\in G\,|\,k\in K\}\\K\cdot a&:=\{k\cdot a\in G\,|\,k\in K\}\\K\cdot L&:=\{k\cdot l\in G\,|\,k\in K\wedge l\in L\}\\K^{-1}&:=\left\{k^{-1}\in G\,|\,k\in K\right\}\end{aligned}$$

と書き表すことにします．

定義 4.2.5 左剰余類

定理 4.2.3 の $\sim$ による G の同値類を，G の H による**左剰余類**と呼びます．

定理 4.2.6

群 $(G,\cdot)$ を群 $(G,\cdot)$ の部分群，集合 A を G の H による左剰余類のひとつとします．このとき，A 内から任意の代表元 a を選ぶと，$A=a\cdot H$ が成り立ちます．

証明　まず $A\subseteq a\cdot H$ を示します：　$b\in A$ と仮定すると $a\sim b$ であり，$\sim$ の定義より $a^{-1}\cdot b\in H$．よって $a\cdot H\ni a\cdot\left(a^{-1}\cdot b\right)=b$ であり，$b\in A\Rightarrow b\in a\cdot H$ が成り立ちます．

次に $a\cdot H\subseteq A$ を示します：　$b\in a\cdot H$ と仮定すると，$b=a\cdot h$ なる $h\in H$ が存在します．この h を用いると $a^{-1}\cdot b=a^{-1}\cdot(a\cdot h)=h$ より $a^{-1}\cdot b=h\in H$，すなわち $\sim$ の定義より $a\sim b$ であり，$b\in A$ が成り立ちます．

以上より $A\subseteq a\cdot H$ かつ $a\cdot H\subseteq A$ であり，$A=a\cdot H$ が成り立ちます．　■

定義 4.2.7 右剰余類

定理 4.2.3 と同様に

$$\forall x\forall y\in G\left(x\sim y\Leftrightarrow x\cdot y^{-1}\in H\right)$$

で定義すると，この関係 $\sim$ は G 上の同値関係となり，$\sim$ による同値類を**右剰余類**と呼びます．

定理 4.2.8

$(H,\cdot)$ が有限群 $(G,\cdot)$ の部分群ならば，$|H|$ は $|G|$ の約数．

証明　（今のところ省略）

4.3 巡回群

定義 4.3.1 内算法の指数表示

$(G,\cdot)$ を群とし，$x\in G$，$n\in\mathbf{N}^+$ に対して $x^0:=e$，$x^n:=x^{n-1}\cdot x$ で指数表示を帰納的に定義します．また $x^{-n}:=\left(x^{-1}\right)^n$ で負整数についても定義します．

補足

逆元の表記 x^{-1} は指数表示の形式と同一で，結果的に同一視できますが，定義上は指数表示よりも逆元の方が先行しています．

定義 4.3.2 巡回群

$(G,\cdot)$ を群とします．

$$\exists x\in G,\exists n\in\mathbf{N}^+\left(\left\{e,x,x^2,\ldots,x^n\right\}=G\right)$$

が成り立つとき，$(G,\cdot)$ を**巡回群**と呼びます．

定理 4.3.3

$(G,\cdot)$ が巡回群ならば，$(G,\cdot)$ は可換群．

証明　自明. ■

定理 4.3.4

巡回群 $(G,\cdot)$ の部分群 $(H,\cdot)$ は巡回群.

証明　群 $(G,\cdot)$ の生成元を a とすると，$H\subseteq G$ より任意の H の元は $n\in\mathbf{N}$ を用いて a^n の形で表せます．また，$a^k\in H$ となる最小の $k\in\mathbf{N}^+$ を考えます．いま $a^n\in H$ と仮定すると，$q\in\mathbf{N}$，$r\in\{0,1,\ldots,k-1\}$ を用いて $n=qk+r$ と一意的に表せて，$a^n=a^{qk+r}=\left(a^k\right)^q\cdot a^r$ より

$$a^r=(a^n)\cdot((a^k)^q)^{-1}$$

であり，$a^k\in H$，$a^n\in H$ および $(H,\cdot)$ が部分群であることより $a^r\in H$ が成り立ちます．k の定義より $a,a^2,\ldots,a^{k-1}\notin H$ であり，したがって $r=0$ が成り立ちます．これより H の元はいずれも $\left(a^k\right)^q$ の形で書くことができ，すなわち $(H,\cdot)$ は a^k を生成元とする巡回群となっています. ■

定義 4.3.5 位数

$(G,\cdot)$ を群とします．$x\in G$ に対して $x^n=e$ を満たす $n\in\mathbf{N}^+$ のうち最小のものを x の**位数**と呼びます.

定理 4.3.6

有限群 $(G,\cdot)$ の任意の元の位数は $|G|$ の約数.

証明　G の元 x の位数を k とし，$(H,\cdot)$ を x を生成元とする巡回群とします．すなわち $H=\bigcup_{i=0}^{k}\left\{x^i\right\}=\left\{e,x,x^2,\ldots,x^{k-1}\right\}$ であり $|H|=k$ が成り立ちます．このとき $(H,\cdot)$ は $(G,\cdot)$ の部分群であり，定理 4.2.8 より $|H|$ は $|G|$ の約数なので，k は $|G|$ の約数. ■

定理 4.3.7

$(G,\cdot)$ を有限可換群とし，G の元 a，b の位数 m，n が互いに素であるならば，$a\cdot b$ の位数は mn.

証明　$a\cdot b$ の位数を k とおきます．まず

$$(a\cdot b)^{mn}=(a^m)^n\cdot(b^n)^m=e^n\cdot e^m=e$$

より mn は k の倍数，すなわち $k\mid mn$ が成り立ちます．一方 $e=(a\cdot b)^k=a^kb^k$ より $a^k=\left(b^k\right)^{-1}=b^{-k}$ であり，これより

$$\left(a^k\right)^n=\left(b^{-k}\right)^n=(b^n)^{-k}=e^{-k}=e$$

であり $m\mid kn$．同様に

$$\left(b^k\right)^m=\left(a^{-k}\right)^m=(a^m)^{-k}=e^{-k}=e$$

であり $n\mid km$．m と n は互いに素なので，これらより $mn\mid k$ が成り立ちます．ゆえに $k\mid mn$ かつ $mn\mid k$ より $k=mn$. ■

定理 4.3.8

$(G,\cdot)$ を有限可換群とし，G の元の位数の最大値を m とおくと，G の任意の元の位数は m の約数．

証明　y を最大の位数 m を持つ G の元とし，任意にとった G の x の位数を n として，背理法によって示します．いま n が m の約数でないとすると，$p^s \mid n$ かつ $p^{s-1} \mid m$ かつ $p^s \nmid m$ なる素数 p と自然数 s が存在します．このような p と s をとって

$$m' := \frac{m}{p^{s-1}} \qquad n' := \frac{n}{p^s} \qquad y' := y^{p^{s-1}} \qquad x' := x^{n'}$$

でそれぞれ定めると，y' の位数は m'，x' の位数は p^s となります．ここで m' と p^s は互いに素なので，定理 4.3.7 より $x'y'$ の位数は $m'p^s = mp$．しかし $mp > m$ より，これは m が最大の位数であることに反し矛盾します．よって n は m の約数であり，G の任意の元の位数は m の約数．■

4.4 正規部分群

定義 4.4.1　正規部分群

群 $(G,\cdot)$ の部分群 $(H,\cdot)$ が

$$\forall x \in G\left(x \cdot H \cdot x^{-1} = H\right)$$

を満たすとき，$(H,\cdot)$ を $(G,\cdot)$ の**正規部分群**と呼びます．

補足

まず記法の話ですが $x \cdot H \cdot x^{-1} = (x \cdot H) \cdot x^{-1} = x \cdot \left(H \cdot x^{-1}\right) = \left\{x \cdot h \cdot x^{-1} \mid h \in H\right\}$ であり，集合に対しても結合律と同様の感覚で扱えます．また $x \cdot H \cdot x^{-1} = H \Leftrightarrow x \cdot H = H \cdot x$ より，

$$\forall x \in G(x \cdot H = H \cdot x)$$

と定義してもよく，結局正規部分群とはそれによる左剰余類と右剰余類が一致する部分群である，ということが言えます．

定義 4.4.2　剰余類

$(G,\cdot)$ を群，$(H,\cdot)$ をその正規部分群とすると，定義より G の H による左剰余類と右剰余類は一致し，これらをまとめて**剰余類**と呼びます．また G の H による剰余類全体は，内算法 $\cdot$ を省略して G/H と書きます．

!!!!要加筆!!!!

索引