数学の基礎 1　集合論・初級編 3

同値関係

東北大学データ駆動科学・AI 教育研究センター

最終更新: 2025 年 9 月 24 日

この巻で学習することの概要

数学で関係 (二項関係) と言えば, 例えば

- $\mathbb{Z}$ 上での約数・倍数の関係 (整除関係): $3|6$, $4 \nmid 7$, ….
- $\mathbb{R}$ 上での大小関係: $2 < 3$, $3 \not\leq 1$, …
- 冪集合 $2^{\mathbb{Z}}$ 上での包含関係: $\{1,2\} \subseteq \{1,2,3\}$, $\{1,2\} \not\subseteq \{2,3,4\}$, …

のように, 2 つの元の間に成立するまたは成立しないという判断にかかる条件を指している. 本巻と次巻では, このような関係に関する基本的な概念を学習する. 特に,「同値関係」「順序関係」と呼ばれる種類の関係は数学の中で幅広く用いられている重要な概念であり, 数学を学ぶ際にはこれらに関する基本的な用語などの知識が必要不可欠である. 関係論では, 新しい言葉がたくさん出てくるので, 面くらわず, かつ正確に理解しておくことが大切である. 本巻では主に同値関係について学習し, 順序関係については次巻で扱う.

Keywords　関係, 反射性, 推移性, 対称性, 反対称性, 同値関係, 同値類と同値類分割, 商集合, 商写像

予備知識　第 1 巻『集合と論理』と第 2 巻『写像』の内容を理解していること.

Contents

1　関係論への導入

1.1　関係の定義

X, Y を任意の集合とする. 後で重要なのは $X = Y$ の場合だが, しばらくは $X \neq Y$ でも差し支えない.

X, Y 上の**関係**, あるいはより詳しく**二項関係**とは, 大雑把に言えば, 任意の $x \in X$ と $y \in Y$ が与えられたとき, それらの間に「成立する」あるいは「成立しない」という判断ができる何らかの基準のことである. 例えば, 図 1 を見てみよう. X は宮城, 埼玉, 山梨, 大阪, 鳥取, 福岡の 6 つの府県から成る集合とし, Y は図の中に描かれているように,「海がある」「近畿地方」などの 5 つの項目から成る集合とする. そして, $x \in X$ と $y \in Y$ に対して, x について y が当てはまっているときには両者を線で結び, そうでなければ結ばないようにすると, 図 1 のようになる.[*1] これは写像に似ている気もするが, 例えば次の 2 点に関して写像にはない現象が起こっている.

- $x =$ 宮城 に対して,「海がある」「新幹線がある」のように, 複数の y が対応している.
- $x =$ 山梨 に対して, 対応する y が全くない.

このような現象が許されるので, 関係は写像に比べて制約が緩い概念だと言える.

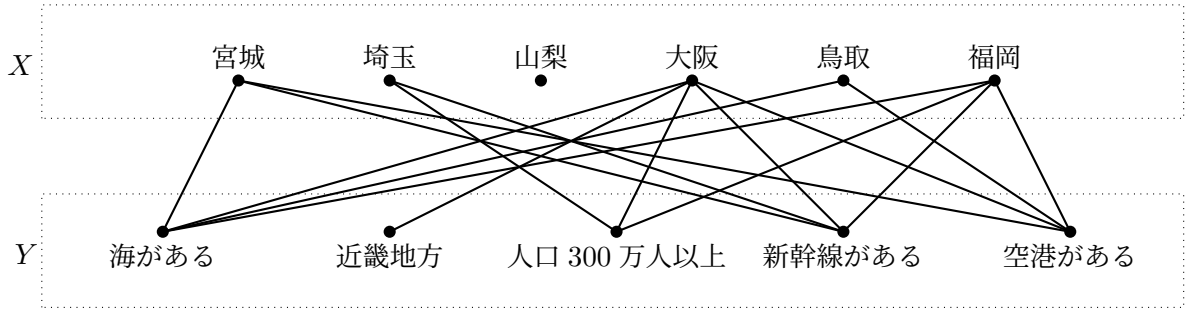


図 1　X と Y の間の関係の例.

図 1 のように, $x \in X$ と $y \in Y$ を線で結ぶ, あるいは結ばないという図を描いたとき, 線で結ばれた組 (x, y) の全体 R を考えれば, これは直積集合 $X \times Y$ の部分集合をなしている. 例えば, (宮城, 海がある) や (福岡, 新幹線がある) は R に所属しているが, (山梨, 海がある) は R に所属していない, という具合である.

逆に, $X \times Y$ の部分集合 R が与えられたとき, $(x, y) \in R$ のとき x と y を線で結び, そうでないときには結ばないと考えれば, この規則が X, Y 上の一つの関係を与えていると考えることもできる. すなわち, これは単に「$(x, y) \in R$ である」という条件を満たすかどうかが判断基準になっている関係である.

[*1] 2025 年現在の状況をもとに記述している.

このように, 抽象的な立場から見れば, X, Y **上の関係とは, 直積集合** $X \times Y$ **の任意の部分集合のことである**という捉え方ができる. これは, 図 1 のようにあらかじめ何らかの意味を持つ関係が想定されていて, そこから $X \times Y$ の部分集合が定まるという理解の仕方ではなくて, そもそも $X \times Y$ の部分集合それ自体が一つの関係を定めていると見なすという考え方である.

X, Y 上の関係のことを, X の元 x と Y の元 y を変数に持つ命題関数と理解することもできる. 写像を用いて説明すれば, これは直積集合 $X \times Y$ から集合 $\{0,1\}$ への写像

$$\pi : X \times Y \to \{0,1\}$$

のことであると理解できる. つまり, (x,y) が成り立っているときには $\pi(x,y) = 1$, 成り立っていないときには $\pi(x,y) = 0$ であると考えるのである. なお, ここで $\{0,1\}$ を用いているのは, 0 を不成立, 1 を成立を表すシンボルとしてそれぞれ用いただけのことであり, $\{\mathrm{YES}, \mathrm{NO}\}$, $\{\mathrm{TRUE}, \mathrm{FALSE}\}$ など, 他の 2 元集合を用いてもよい. 関係を $X \times Y$ から $\{0,1\}$ への写像 π として表現すれば, そこから $X \times Y$ の部分集合

$$R = \pi^{-1}(1) = \{(x,y) \mid \pi(x,y) = 1\}$$

が定まる. 逆に, $X \times Y$ の部分集合 R が与えられたとき, 写像 $\pi : X \times Y \to \{0,1\}$ を

$$\pi(x,y) = \begin{cases} 1 & ((x,y) \in R \text{ であるとき}) \\ 0 & ((x,y) \notin R \text{ であるとき}) \end{cases}$$

で定めれば, 写像としての関係 π が復元できる. このように, 形式的には, X, Y 上の関係のことを, 次のどちらの方法で理解しても実質的には同じことだと考えてよい:

- 直積 $X \times Y$ の部分集合.
- 直積 $X \times Y$ から集合 $\{0,1\}$ への写像.

♦ **例 1.1**　$f : X \to Y$ を X から Y への写像とするとき, それのグラフ

$$R = \{(x,y) \in X \times Y \mid y = f(x)\}$$

は直積 $X \times Y$ の部分集合であり, X, Y 上の関係を与えている. これはもちろん, $y = f(x)$ が成り立っているかどうかが判断基準となっている関係である. □

さらに一般的に, 3 つ以上の集合 $X_1, \ldots, X_n$ に対して, 直積 $X_1 \times \cdots \times X_n$ から $\{0,1\}$ への写像, あるいはそれに対応する $X_1 \times \cdots \times X_n$ の部分集合のことを $X_1, \ldots, X_n$ 上の n**-項関係**と言う. 本巻の中ではもっぱら $n = 2$ の場合のみを考察する.

1.2　関係の演算と合成

集合 X, Y 上の関係は, 抽象的には直積集合 $X \times Y$ の部分集合と考えることができるので, 関係に対して包含関係を考えたり, 集合の和, 共通部分, 差, 対称差などの集合演算を適用することができる.

さらに, 関係は写像の一般化とも考えられるから, 写像の合成と同じようにして関係の合成を考えることもできる. X, Y, Z を集合, $R_1 \subseteq X \times Y$, $R_2 \subseteq Y \times Z$ とするとき,

$$R = \{(x,z) \in X \times Z \mid \text{ある } y \in Y \text{ が存在して, } (x,y) \in R_1 \text{ かつ } (y,z) \in R_2 \text{ となる}\}$$

で定義される関係 $R \subseteq X \times Z$ を R_1 と R_2 の**合成**と言い, $R = R_2 \circ R_1$ で表す. 写像としての言葉で表現すれば, $R = R_2 \circ R_1$ は

$$R(x,z) = \begin{cases} 1 & (R_1(x,y) = R_2(y,z) = 1 \text{ となる } y \in Y \text{が存在するとき}) \\ 0 & (\text{それ以外のとき}) \end{cases}$$

で定まる写像 $R : X \times Z \to \{0,1\}$ として書ける. 図 2 では, y_4 を仲介役として赤線を辿れば $(x_3, z_1) \in R_2 \circ R_1$ であることがわかるし, y_1 を仲介役として青線を辿っても $(x_3, z_1) \in R_2 \circ R_1$ であることがわかる. $(x_6, y) \in R_1$ かつ $(y, z_4) \in R_2$ となる y は存在しないので, $(x_6, z_4) \notin R_2 \circ R_1$ である.

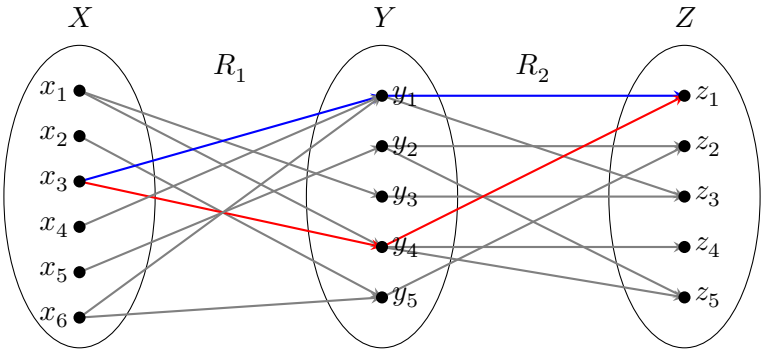


図 2　合成 $R_2 \circ R_1$.

♦ **例 1.2**　X を料理の集合, Y を食材の集合, Z を栄養素の集合として, 関係 R_1, R_2 をそれぞれ

$$R_1 = \{(x,y) \in X \times Y \mid y \text{ は } x \text{ の材料である}\}$$
$$R_2 = \{(y,z) \in Y \times Z \mid z \text{ は } y \text{ に豊富に含まれている}\}$$

とする. このとき, 合成関係 $R = R_2 \circ R_1$ は「料理 x を食べると, 栄養素 z をたくさん摂取できる」という組 (x,z) らから成る関係である. 例えば, 肉じゃがにはニンジンが入っていて, ニンジンには β-カロテンが豊富に含まれているので, つまり (肉じゃが, ニンジン) $\in R_1$, (ニンジン, β-カロテン) $\in R_2$ なので, 肉じゃがを食べると β-カロテンを摂取できる (つまり, (肉じゃが, β-カロテン) $\in R$) というわけである. 一方で, 例えば肉じゃがに含まれている食材の中に亜鉛を含んでいるものが全くないという場合は, 肉じゃがを食べても亜鉛を摂取できないので, (肉じゃが, 亜鉛) $\notin R$ である. □

任意の集合 X 上で,

$$\Delta_X \stackrel{\text{def}}{=} \{(x,x) \mid x \in X\} \tag{1}$$

で定義される関係 Δ_X は見た通り等号の関係であり, $(x,x') \in \Delta_X$ であるのは $x = x'$ である場合に限られる. これは恒等写像 ϵ_X のグラフであり, 恒等写像を X 上の関係として表現したものだとも考えられる. 任意の関係 $R \subseteq X \times Y$ に対して,

$$R \circ \Delta_X = R, \quad \Delta_Y \circ R = R$$

が成り立つが, これは任意の写像 $f : X \to Y$ について $f \circ \epsilon_X = f$, $\epsilon_Y \circ f = f$ が成り立つことの類似である. さらに, 関係 $R \subseteq X \times Y$ に対して,

$$R^{-1} \stackrel{\text{def}}{=} \{(y,x) \in Y \times X \mid (x,y) \in R\} \tag{2}$$

で定義される関係 $R^{-1} \subseteq Y \times X$ を R の**逆関係**と言う．これは写像に対する逆写像に相当するものだが，逆写像は全単射に対してのみ定義できることに対して，逆関係は任意の関係に対して定義できる．定義から明らかなように，R^{-1} の逆関係は R 自身である．つまり，$(R^{-1})^{-1} = R$ である．

▶ **演習 1.1** (合成の結合則)　A, B, C, D を集合，$R_1 \subseteq A \times B$, $R_2 \subseteq B \times C$, $R_3 \subseteq C \times D$ とするとき，

$$(R_3 \circ R_2) \circ R_1 = R_3 \circ (R_2 \circ R_1)$$

であることを証明せよ．

▶ **演習 1.2**　X, Y, Z を集合，$R_1 \subseteq X \times Y$, $R_2 \subseteq Y \times Z$ とするとき，

$$(R_2 \circ R_1)^{-1} = R_1^{-1} \circ R_2^{-1}$$

であることを証明せよ．

▶ **演習 1.3**　任意の $R \subseteq X \times Y$ に対して，$R \circ R^{-1} = \Delta_X$, $R^{-1} \circ R = \Delta_Y$ はそれぞれ成立するか? 成立するならばそのことを証明して，そうでないならば具体的な反例を与えよ．

▶ **演習 1.4**　$R, R' \subseteq X \times Y$ とするとき，次のことをそれぞれ示せ．

(1) $R \subseteq R'$ ならば $R^{-1} \subseteq R'^{-1}$ である．
(2) $(R \cap R')^{-1} = R^{-1} \cap R'^{-1}$ である．
(3) $(R \cup R')^{-1} = R^{-1} \cup R'^{-1}$ である．

1.3　関係の基本的な性質

本項では，もっぱら一つの集合 X 上で定義される二項関係，すなわち $X^2 = X \times X$ の部分集合として表される二項関係についてのみ考える．

数学でよく出てくる関係は，当然と言えば当然であるが，ある程度整った性質を持ったものである．ここでは，最もよく引用される 4 つの基本的な性質を挙げておく．式を見やすくするために，一般に関係 R について $(x, y) \in R$ であることを xRy と書く．場合によっては，$x \simeq y$, $x \equiv y$, $x \leq y$ などのように何らかの特別な記号を用いることもある．

関係の代表的な基本性質

定義 1.3. R を X 上の関係とする．

(1) R が**反射的** $\overset{\text{def}}{\iff}$ xRx である．
(2) R が**対称的** $\overset{\text{def}}{\iff}$ xRy であれば yRx でもある．
(3) R が**反対称的** $\overset{\text{def}}{\iff}$ xRy かつ yRx ならば $x = y$ である．
(4) R が**推移的** $\overset{\text{def}}{\iff}$ xRy かつ yRz ならば xRz である．

ただし，x, y, z は X の任意の元を表す．

これらの性質は，次のように手短に言い換えることもできる．

- R が反射的 $\iff \Delta_X \subseteq R$.
- R が対称的 $\iff R^{-1} \subseteq R \iff R = R^{-1}$.
- R が推移的 $\iff R \circ R \subseteq R$.
- R が反対称的 $\iff R \cap R^{-1} \subseteq \Delta_X$.

ここで, Δ_X は式 (1) で定義した等号関係である.

♦ **例 1.4**　(1) $\mathbb{Z}$ 上で通常の大小関係 $\leq$ は反射的, 反対称的かつ推移的であるが, 対称的ではない. 例えば, $3 \leq 5$ であるが, $5 \leq 3$ ではない.

(2) $\mathbb{Z}$ 上で, 整除関係は反射的かつ推移的である. $4|8$ であるが $8|4$ ではないので, 対称性は破れている. $5|-5$ かつ $-5|5$ だが $5 \neq -5$ なので, 反対称性も破れている. (ただし, 数の範囲を $\mathbb{Z}$ ではなく $\mathbb{N}$ に制限しておけば, 反対称性は破れない.)

(3) $\mathbb{Z}$ 上の関係 $\sim$ を「$x \sim y \overset{\text{def}}{\iff} x+y$ は偶数である」という規則で定める. この関係は反射的, 対称的かつ推移的であるが, 反対称的ではない. □

♦ **例 1.5**　$\mathbb{N}$ 上で次の関係 $\sim$ が定義 1.3 の 4 条件のうちどれを満たすかを調べてみよう.

$$x \sim y \overset{\text{def}}{\iff} \text{ある } a, b \in \mathbb{N} \text{ が存在して } x^a | y^b \text{ である.} \tag{3}$$

反射性: 任意の $x \in \mathbb{N}$ について $x^1 | x^1$ だから, $x \sim x$ である. (式 (3) で $x = y$, $a = b = 1$ の場合を考えた.) よって, $\sim$ は反射的である.

対称性: $x = 12 = 2^2 \times 3$, $y = 90 = 2 \times 3^2 \times 5$ とすると, $a = 1$, $b = 2$ に対して $x^a | y^b$ だから $x \sim y$ である. しかし, どんな $a, b \in \mathbb{N}$ についても $y^b | x^a$ とはならない. y^b は 5 の倍数であるが, x^a は 5 を素因数として持たないからである. ゆえに, $y \sim x$ は成立しない. したがって, $\sim$ は対称的ではない.

反対称性: $x = 12 = 2^2 \times 3$, $y = 2 \times 3^2 = 18$ とすると, $x | y^2$ かつ $y | x^2$ だから, $x \sim y$ と $y \sim x$ はどちらも成立する. しかし, $x \neq y$ である. だから, $\sim$ は反対称的ではない.

推移性: $x \sim y$ かつ $y \sim z$ とすると, ある自然数 $a, b, c, d \in \mathbb{N}$ が存在して $x^a | y^b$ かつ $y^c | z^d$ である. このとき $x^{ac} | z^{bd}$ だから, $x \sim z$ である. ゆえに, $\sim$ は推移的である. □

▶ **演習 1.5**　次の各関係について, 例 1.5 に倣って, それが定義 1.3 の 4 条件のうちどれを満たすかを論ぜよ.

(1) X を $\mathbb{Z}$ の空でない部分集合の全体, $A, B \in X$ とするとき, $A \sim B \overset{\text{def}}{\iff} A \cap B \neq \emptyset$.

(2) X を 0 以外の実数の全体, $x, y \in X$ とするとき, $x \sim y \overset{\text{def}}{\iff} x/y \in \mathbb{Q}$.

▶ **演習 1.6**　次のような関係の具体例を挙げよ.

(1) 対称的かつ推移的であるが, 反射的ではない.

(2) 反射的かつ対称的であるが, 推移的ではない.

(3) 反射的かつ推移的であるが, 対称的ではない.

▶ **演習 1.7**　(1) 対称的かつ反対称的であるが, 反射的ではない関係の具体例を作れ.

(2) 対称的かつ反対称的な関係は反射的であることを, 次のように証明した.

誤証明: $x \in X$ とする. $x \sim y$ となる任意の $y \in X$ を選ぶと, $\sim$ は対称的なので $y \sim x$ でもある. したがって, $\sim$ の反対称性から $x = y$ となる. ゆえに, $x \sim x$ である. 以上から, $\sim$ は反射

的である.

しかし, (1) のような事例があるので, この証明は間違っている. どこが間違っている?

1.4　グラフによる関係の図示

集合上の二項関係を視覚的に図示するために, グラフ構造がしばしば利用される. **グラフ**とは, 次の図 3 の通りいくつかの点が線で結ばれている組み合わせ構造のことを言うが, これは「関数のグラフ」と言うときのグラフとは全く別の概念である. 抽象的には, グラフは**点集合** V と**辺集合** E との組 $G = (V, E)$ として定義される. V と E が有限集合であるグラフを**有限グラフ**と言い, そうでないグラフは**無限グラフ**と呼ばれる. E の各々の元 e, すなわち G の辺には 2 つの点 $x, y \in V$ から成る組 (x, y) が割り振られていて, x, y を辺 e の**端点**と呼ぶ. この組 (x, y) を順序組と見なせば, 辺 e には x から y へ**向き**が指定されていると考えることができる. 組 (x, y) を非順序組と見なせば, 辺 e には特定の向きはないと考えられる. 各々の辺 $e \in E$ に向きが指定されたグラフを**有向グラフ**と言い, 辺に特定の向きを考慮しないグラフを**無向グラフ**と呼ぶ.

図 3 は 8 個の点を持つ無向グラフを描いている. なお, 形式的にはグラフとはあくまで点集合 V と辺集合 E の組 $G = (V, E)$ のことであり, 図はそれを可視化したものという考え方をとる. 同じグラフが描き方によっては全く異なる図として描かれることもある. 例えば, 図 3 でも点 x_4 を右上側に移動させると見かけはがらっと変わるだろうが, それでもグラフ自身が変わるわけではない.

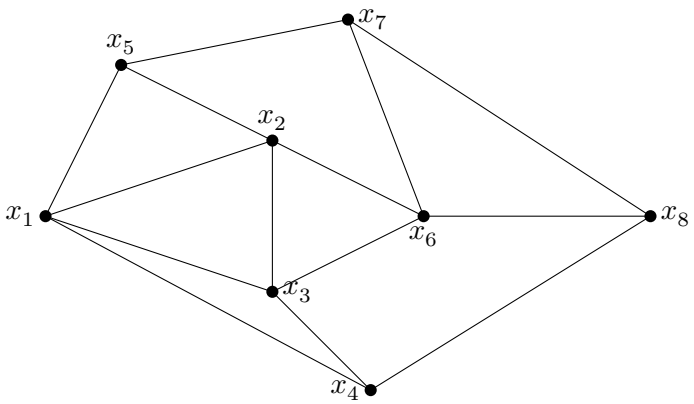


図 3　8 個の点を持つ無向グラフの例.

グラフ G 上の**道**とは, ある点 x から出発して G 上の辺を有限本辿りつつ点 y に到達する経路のことを言う.[*2] (出発点 x と終着点 y が同じ点であってもよい.) 形式的には, そのような経路は有限個の辺から成る列 $e_1, e_2, \ldots, e_m$ で, 全ての $1 \leq i \leq m$ について

$$e_{i-1} \text{ の終点} = e_i \text{ の始点}$$

が成り立つものとして定義できる. 有向グラフ上では辺の向きに逆らって進むことはできないが, 無向グラフ上では辺の向きを気にする必要はなく, どの辺も双方向に進むことができる. 道は同じ辺を複数回通ってもよいが, そのような道は適当に簡略化することで同じ辺を 2 度以上通らない短い道に作り替えることもできる.

[*2] グラフ関係の用語には, 文献によって細かい違いがあることがあるので, 他の文献などを参照する場合には要注意である. 例えば,「道」にしても, それが同じ辺を複数回通るかどうか, 同じ点を複数回通るかどうかなどの事情によって細かく用語を使い分けることもある.

集合 X 上に二項関係 R が設定されたとき, X を点集合とし, R を辺集合とする有向グラフ G を考えることができる. R が反射的ならば, どの点 $x \in X$ のまわりにも x を両端点とする辺 (x における**ループ辺**) が描かれることになるが, R が反射的という了解の下ではそのような辺を省略して図を簡略化できる. R が対称的ならば, 辺 $x \to y$ があれば必ず逆向きの辺 $y \to x$ があるので, G を有向グラフではなく無向グラフとして描くことが普通である. (辺 $x \to y$ と $y \to x$ をひとまとめにして一本の無向辺と見なす.) R が推移的ならば, 本来であれば辺 $x \to y$ と $y \to z$ があれば辺 $x \to z$ を必ず描くことになるが, そうすると辺が増えすぎて図が煩雑になるので, 推移性を用いて他の辺から補完できる辺は描かないようにすることもできる. 例えば, 図 3 が集合 $X = \{x_1, x_2, \dots, x_8\}$ 上の反射的, 対称的かつ推移的な関係 R を図示していると考えれば, R は次の 3 種類の組から構成される関係だと読み取れる:

- 各点 $x \in X$ に対する組 (x, x).
- 各々の無向辺に対する組. 例えば, x_1 と x_5 を結ぶ辺は $(x_1, x_5) \in R$ および $(x_5, x_1) \in R$ であることを示している.
- 各々の道に対する組. 例えば, 道 $x_1 \to x_4 \to x_8 \to x_6$ を取れば, $(x_1, x_4) \in R$, $(x_4, x_8) \in R$ かつ $(x_8, x_6) \in R$ だから, R の推移性でこれらを繋げば $(x_1, x_6) \in R$ であることが読み取れる. 同時に, 対称性から $(x_6, x_1) \in R$ であることも言える.

1.5　関係の閉包

R を集合 X 上の二項関係とする. $\Delta = \Delta_X$ を式 (1) で定義した等号関係として

$$R_{\mathrm{ref}} \stackrel{\text{def}}{=} R \cup \Delta$$

と定める. これは Δ を含むから反射的である. R' が R を含む反射的な関係ならば, $R \subseteq R'$ かつ $\Delta \subseteq R'$ となるので, $R_{\mathrm{ref}} \subseteq R'$ となる. したがって, R_{ref} は R を含む反射的な関係のうちで**最小**のものである. これを R の**反射閉包**と呼ぶ. 定義から $R \subseteq R_{\mathrm{ref}}$ であるが, R 自身が反射的であるとき, かつその時に限り, $R = R_{\mathrm{ref}}$ である. 特に, $(R_{\mathrm{ref}})_{\mathrm{ref}} = R_{\mathrm{ref}}$ である.

同じように, 対称性についても閉包を作ってみよう. R に対して

$$R_{\mathrm{sym}} \stackrel{\text{def}}{=} R \cup R^{-1}$$

と定める. 演習 1.4(3) から,

$$R_{\mathrm{sym}}^{-1} = (R \cup R^{-1})^{-1} = R^{-1} \cup (R^{-1})^{-1} = R^{-1} \cup R = R_{\mathrm{sym}}$$

だから, R_{sym} は対称的である. 一方, R' が R を含む対称的な関係ならば, $R \subseteq R'$ から $R^{-1} \subseteq R'^{-1}$ でもあり (→演習 1.4(1)), $R_{\mathrm{sym}} = R \cup R^{-1} \subseteq R'$ となる. よって, R_{sym} は R を含む対称的な関係のうちで最小のものである. これを R の**対称閉包**と言う. 定義から $R \subseteq R_{\mathrm{sym}}$ であるが, R が対称的であるとき, かつその時に限り, $R = R_{\mathrm{sym}}$ である. 特に, $(R_{\mathrm{sym}})_{\mathrm{sym}} = R_{\mathrm{sym}}$ である.

ここまで, R の反射性と対称性に関する閉包を見てきたが, 推移性に関してはどうだろうか. 実は推移性についても同様に, R を含む推移的な関係として最小のものを構成することができて, それを R の**推移閉包**と呼ぶ. R の推移閉包は次のようにして構成することができる. X 上の **R-鎖**とは, 有限個の点から成る順序列 $x_0, x_1, \dots, x_n$ で全ての $1 \leq i \leq n$ に対して $(x_{i-1}, x_i) \in R$ が成り立つものを言う. そして,

$$R_{\mathrm{trans}} \stackrel{\text{def}}{=} \{(x, y) \in X^2 \mid x \text{ から } y \text{ への } R\text{-鎖が存在する}\}$$

とおく.

補題 1.6. R_{trans} は R を含む推移的な関係である.

証明. 任意の $(x,y) \in R$ について, x, y は R-鎖なので, $(x,y) \in R_{\mathrm{trans}}$ である. よって, $R \subseteq R_{\mathrm{trans}}$ である. R_{trans} の推移性を示そう. $(x,y),(y,z) \in R_{\mathrm{trans}}$ を仮定して, $(x,z) \in R_{\mathrm{trans}}$ であることを示せばよい. $(x,y),(y,z) \in R_{\mathrm{trans}}$ だから, それぞれ x から y への R-鎖 α と y から z への R-鎖 β が存在する. α の直後に β を繋げば, x から y を通って z へ至る R-鎖が得られるので, $(x,z) \in R_{\mathrm{trans}}$ である. □

これで R_{trans} が R を含む推移的な関係であることがわかった. S が R を含む推移的な関係であるとする. 任意の $(x,y) \in R_{\mathrm{trans}}$ を考え, x から y へ至る R-鎖 $x = x_0, x_1, \ldots, x_n = y$ を取る. 任意の $1 \leq i \leq n$ について $(x_{i-1}, x_i) \in R \subseteq S$ なので, S の推移性を繰り返し使えば $(x,y) = (x_0, x_n) \in S$ を得る. よって, $R_{\mathrm{trans}} \subseteq S$ である. これで R_{trans} が R を含む最小の推移的関係, すなわち R の推移閉包であることが言えた.

補足 1.7　関係 R の推移閉包を求めるには次のような簡単な方法もある. X 上で R を含む推移的な関係の全体を $\mathcal{R} = \{R_i\}_{i \in I}$ とする. これは $X \times X$ を含むから空集合ではない. 全ての R_i に渡る共通部分を $\bar{R} = \bigcap_{i \in I} R_i$ とする. どの R_i も R を含むから, $R \subseteq \bar{R}$ である. $(x,y),(y,z) \in \bar{R}$ とすると, どの $i \in I$ についても $(x,y),(y,z) \in R_i$ であるが, R_i は推移的なので $(x,z) \in R_i$ であり, したがって $(x,z) \in \bar{R}$ も成り立つ. よって, $\bar{R}$ は推移的である. R' が R を含む推移的な関係であれば, ある i について $R' = R_i$ なので, $\bar{R} \subseteq R_i = R'$ である. したがって, $\bar{R}$ は R を含む最小の推移的関係, すなわち R の推移閉包である.

この構成法は,「推移的である」という性質が共通部分を取る操作で保存されることを利用している. この構成は簡潔なのは利点だが, 完成品たる $\bar{R}$ の実体がよく見えないのが欠点である. 実際に推移閉包を用いる議論では, 先に説明した構成的な手法の方が閉包の実体がよく見えて有用である. □

関係 R に対して, その推移閉包 R_{trans} を対応づける規則については次のことが成り立つ.

- 拡張性: R_{trans} は R を含む推移的関係であり, $R \subseteq R_{\mathrm{trans}}$ である.
- 単調性: $R \subseteq R'$ ならば, $R \subseteq R' \subseteq R'_{\mathrm{trans}}$ だから R'_{trans} は R を含む推移的関係であるが, R_{trans} はそのような最小の推移的関係なので, $R_{\mathrm{trans}} \subseteq R'_{\mathrm{trans}}$ である.
- 冪等性: R_{trans} は推移的だから, それを含む最小の推移的関係はそれ自身である. ゆえに, $(R_{\mathrm{trans}})_{\mathrm{trans}} = R_{\mathrm{trans}}$ である.

反射閉包や対称閉包についても同様のことが言える.

ここまで, 意識的に反対称性に触れることを避けてきたが, 反対称性についても同様に閉包を考えることができるだろうか? 実は, そのようなものを考えても実質的な意味はない. なぜだろう? 反対称性の定義からすぐに分かることだが, 反対称性は部分集合に遺伝する. つまり, $R \subseteq R'$ であり, R' が反対称的ならば, R も反対称的である. ということは, もし関係 R に反対称閉包 (R を含む最小の反対称的関係) が存在するならば, R 自身が反対称的であり, したがって R の反対称閉包は R 自身である. そして, R が反対称的でなければ, R の反対称閉包は存在しない.

▶ **演習 1.8**　X を任意の集合, R を X 上の関係とする. R が対称的ならば, R の推移閉包も対称的であることを示せ.

▶ **演習 1.9**　X を $\mathbb{N}$ の空でない部分集合の全体とする．任意の $x, y \in X$ に対して，$x \sim y$ であることを $x \cap y \neq \emptyset$ であることで定義する．

(1) $\sim$ は推移的**ではない**ことを示せ．
(2) $\sim$ の推移閉包を $\approx$ で表す．どの $x, y \in X$ に対しても，$x \approx y$ が成り立つことを示せ．

2　同値関係と同値類分割

同値関係は等号の関係を一般化したものであり，厳密には互いに異なるものであっても，「細かい違いを無視すれば互いに同一視できる」「ある特定の性質に注目すれば互いに仲間だと思える」という意味を持っている．つまり，**同値関係は集合の元たちをある一定の基準に従って分類するという機能を持つ関係である**．数学では，2 つの対象物の細かい違いには目をつむることで，却って両者に共通な本質的な情報が浮かび上がってくるということがよくあり，そんな時こそ同値関係の出番である．

2.1　同値関係の定義と実例

同値関係

定義 2.1. 反射的，対称的かつ推移的な関係を**同値関係**と言う．

すなわち，集合 X 上に定義された二項関係 $\equiv$ が同値関係であるとは，次の 3 つの要件が満たされていることを言う:

- **反射性**: $x \equiv x$ である．
- **対称性**: $x \equiv y$ ならば，$y \equiv x$ でもある．
- **推移性**: $x \equiv y$ かつ $y \equiv z$ ならば，$x \equiv z$ である．

♦ **例 2.2**　2 次元座標平面 $\mathbb{R}^2$ 上の関係 $\equiv$ を次の式で定める:

$$(x_1, y_1) \equiv (x_2, y_2) \overset{\text{def}}{\iff} x_1^2 + y_1^2 = x_2^2 + y_2^2.$$

これは，$\mathbb{R}^2$ で点 (x_1, y_1) と点 (x_2, y_2) が原点を中心とする同じ半径の円周上に乗ること，つまり原点からの直線距離が同じであることを意味する同値関係である．すなわち，$\equiv$ は平面上の点を原点からの直線距離に応じて分類している．　□

♦ **例 2.3**　$f : X \to Y$ を写像とする．X 上の関係 $\equiv$ を次の式で定める:

$$x \equiv x' \overset{\text{def}}{\iff} f(x) = f(x').$$

これは，X の元を f による像に従って分類する機能を持つ同値関係である．　□

♦ **例 2.4**　$\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$, $Q = \mathbb{Z} \times \mathbb{Z}^*$ とおく．$(a, b), (c, d) \in Q$ のとき，

$$(a, b) \equiv (c, d) \overset{\text{def}}{\iff} ad = bc$$

と定義する．$\equiv$ が反射的かつ対称的であることの検証は容易なので，ここでは推移性のみを示す．$(a,b)\equiv(c,d)$, $(c,d)\equiv(e,f)$ とすると，$ad=bc$ かつ $cf=de$ だから，$(af)d=(ad)f=(bc)f=b(cf)=b(de)=(be)d$ であるが，ここで $d\neq 0$ だから，$af=be$ である．よって，$(a,b)\equiv(e,f)$ である．ゆえに，$\equiv$ は推移的である．したがって，$\equiv$ は Q 上の同値関係である．$(a,b)\equiv(c,d)$ であることは，分数として $a/b=c/d$ であることと同じである．つまり，$\equiv$ は Q の元をそれが表す分数に応じて分類する同値関係である．□

♦ **例 2.5** (整数の合同関係)　n を整数とするとき，任意の $a,b\in\mathbb{Z}$ に対して

$$a\equiv b \overset{\text{def}}{\iff} a-b\in n\mathbb{Z}$$

で定義される関係 $\equiv$ を考える．ここで，$n\mathbb{Z}=\{nk\mid k\in\mathbb{Z}\}$ は n の倍数全体を表す．これを n を法とする**合同関係**と言う．この関係が同値関係であることを示そう．

反射性: 任意の x について，$x-x=0\in n\mathbb{Z}$ だから $x\equiv x$ である．ゆえに，$\equiv$ は反射的である．

対称性: $x\equiv y$ とすると，$x-y\in n\mathbb{Z}$，すなわち，ある整数 k が存在して $x-y=nk$ である．このとき，$y-x=-nk=n(-k)\in n\mathbb{Z}$ だから，$y\equiv x$ でもある．よって，$\equiv$ は対称的である．

推移性: $x\equiv y$, $y\equiv z$ ならば，ある整数 $k,\ell\in\mathbb{Z}$ が存在して $x-y=nk$, $y-z=n\ell$ である．このとき，$x-z=(x-y)+(y-z)=n(k+\ell)\in n\mathbb{Z}$ だから $x\equiv z$ である．ゆえに，$\equiv$ は推移的である．

以上から，$\equiv$ は同値関係である．$n\neq 0$ であるとき，$x\equiv y$ であることは，x と y をそれぞれ n で割ったときの余りが一致することと同じである．すなわち，n を法とする合同関係とは，整数を「n で割った時の余り」という基準で分類する関係である．$n=0$ のときには，$x\equiv y$ は $x=y$ と同じことである．□

♦ **例 2.6**　(この例は線型代数学の知識がある読者向けである.) $M_n(\mathbb{R})$ を $\mathbb{R}$ 上の n 次正方行列の全体とし，その中で特に正則であるものの全体を $\mathrm{GL}_n(\mathbb{R})$ とする．任意の $A,B\in M_n(\mathbb{R})$ に対して次のように定義する:

$$A\equiv B \overset{\text{def}}{\iff} \text{ある } P,Q\in\mathrm{GL}_n(\mathbb{R}) \text{ が存在して } A=PBQ \text{ である.}$$

この関係 $\equiv$ は $M_n(\mathbb{R})$ 上の同値関係であることを示そう．

- 反射性: 任意の $A\in M_n(\mathbb{R})$ について，$P=Q=E$ (単位行列) とすれば $A=PAQ$ が成り立つ．よって，$A\equiv A$ である．
- 対称性: $A\equiv B$ とすると，正則行列 $P,Q\in\mathrm{GL}_n(\mathbb{R})$ が存在して $A=PBQ$ である．$P'=P^{-1}$ と $Q'=Q^{-1}$ も正則行列であり，かつ $B=P'AQ'$ である．よって，$B\equiv A$ でもある．
- 推移性: $A\equiv B$, $B\equiv C$ とすると，ある $P_1,Q_1,P_2,Q_2\in\mathrm{GL}_n(\mathbb{R})$ が存在して，$A=P_1BQ_1$ かつ $B=P_2CQ_2$ である．$P=P_1P_2$ と $Q=Q_2Q_1$ は正則行列どうしの積だから正則行列であり，

  $$A=P_1BQ_1=P_1(P_2CQ_2)Q_1=(P_1P_2)C(Q_2Q_1)=PCQ$$

  である．したがって，$A\equiv C$ でもある．

以上から，$\equiv$ は同値関係である．$A\equiv B$ は A と B の階数が同じという意味であり，$\equiv$ は行列をその階数に従って分類する機能を持っている．□

♦ **例 2.7**　$G=(V,E)$ を無向グラフとする．任意の点 $x,y\in V$ に対して，$x\to y$ であることを G が x から y へ至る道を持つことと定義する．ただし，どの点 $x\in V$ についても，「x から全く動かない」ことを

x から x 自身へ至る ‘長さが 0’ の道と認めることで, $\to$ は反射的であると考えることにする. $x, y \in V$, $x \to y$ であるとき, G 上には x から y へ至る道 p があるが, G **は無向グラフ**だから p を逆順に辿って y から x に行くことができて, したがって $y \to x$ でもある. よって, $\to$ は対称的である. $x, y, z \in V$, $x \to y$ かつ $y \to z$ とするとき, G 上で x から y への道 p と y から z への道 q がそれぞれ存在するが, p を辿って x から y へ行って, そこから続けて q を辿って y から z へ行けば, x から z への道が得られる. (これを p と q を**連接**した道と呼ぶ.) よって, $x \to z$ であり, $\to$ は推移的である. 以上から, $\to$ は V 上の同値関係である.

例えば, 図 3 のグラフ G にこの関係 $\to$ を考えれば, どの 2 点 $x, y \in V$ に対しても $x \to y$ が成り立っているが, このようなグラフ G は**連結**であると言う. これは直観的には, まさに図 3 の通り G が「ひとかたまり」の島からできているという意味である.

G が有向グラフである場合には, $\to$ は必ずしも対称的ではなく, したがって同値関係にならない可能性がある. 例えば, G が 2 個の点 x, y と 1 本の辺 e を持つ有向グラフで, e の向きが x から y への向きであるとき, $x \to y$ ではあるが $y \to x$ は成り立たない. □

▶ **演習 2.1**　(この演習問題は線型代数学の知識がある読者向けである.) 実数成分の n 次正則行列の全体を $\mathrm{GL}_n(\mathbb{R})$ とし, その中でも特に行列式が 1 であるものの全体を $\mathrm{SL}_n(\mathbb{R})$ とする. $\mathrm{GL}_n(\mathbb{R})$ 上の関係 $\equiv$ を次のように定める:

$$A \equiv B \overset{\text{def}}{\iff} \text{ある } S \in \mathrm{SL}_n(\mathbb{R}) \text{ が存在して } A = BS \text{ である.}$$

この関係 $\equiv$ は同値関係であることを示せ.

▶ **演習 2.2**　X を空でない集合, $f : X \to X$ を写像とするとき, X 上で次の式で定義される関係 $\equiv$ は同値関係であることを示せ: $x, y \in X$ のとき,

$$x \equiv y \overset{\text{def}}{\iff} \text{ある自然数 } m, n \text{ が存在して } f^m(x) = f^n(y) \text{ である.}$$

ここで, $f^1 = f$, $f^n = f \circ f^{n-1}$ $(n \geq 2)$ である.

▶ **演習 2.3**　X を任意の集合とし, R を X 上の関係とする.

(1) R に対して, 反射閉包を取る操作と対称閉包を取る操作は, どちらを先にやっても結果は変わらないこと, つまり

$$(R_{\mathrm{ref}})_{\mathrm{sym}} = (R_{\mathrm{sym}})_{\mathrm{ref}}$$

であることを示せ. これは R を含み, かつ反射的かつ対称的な最小の関係であり, R の**反射対称閉包**と呼ぶ.

(2) R の反射対称閉包の推移閉包は R を含む最小の同値関係であることを示せ. この同値関係を R が**生成**する同値関係と呼ぶ.

2.2　同値類と同値類分割

これまで見てきた通り, 同値関係は何らかの基準に従って元を分類する機能を持つ. そのことを一般的に説明してみよう. X を空でない集合とし, $\equiv$ を X 上の同値関係とする.

定義 2.8 (同値類)**.** 元 $x \in X$ について, X の部分集合

$$C_x \stackrel{\text{def}}{=} \{a \in X \mid x \equiv a\}$$

を同値関係 $\equiv$ に関する x の**同値類**と呼ぶ.

$\equiv$ は対称的な関係なので, C_x のことを

$$C_x = \{a \in X \mid a \equiv x\}$$

と書いてもよい.

命題 2.9. x, y を X の任意の元とする.

(1) $x \in C_x$ である. 特に, C_x は空集合ではない.
(2) $x \equiv y \iff C_x = C_y$ である.
(3) $x \not\equiv y \iff C_x \cap C_y = \emptyset$ である.

証明. (1) $\equiv$ の反射性から明らかである.

(2) $x \equiv y$ ならば $C_x = C_y$ であることを示す. $z \in C_x$ とする. すると $x \equiv z$ であるが, これと $x \equiv y$ から, 推移性を使えば $z \equiv y$ を得る. ゆえに, $z \in C_y$ である. よって, $C_x \subseteq C_y$ である. x と y の立場を交換して同様にすれば, $C_y \subseteq C_x$ であることもわかる. 以上から, $C_x = C_y$ である.

逆に, $C_x = C_y$ ならば, $x \in C_x = C_y$ だから $x \equiv y$ である.

(3) 両辺の否定どうしが同値であること, つまり $x \equiv y \iff C_x \cap C_y \neq \emptyset$ を示せばよい.

$x \equiv y$ ならば, (1) と (2) から $C_x \cap C_y = C_x = C_y \neq \emptyset$ である. 次に, $C_x \cap C_y \neq \emptyset$ ならば $x \equiv y$ であることを示す. $z \in C_x \cap C_y$ を任意に選ぶ. $z \in C_x$ だから $x \equiv z$ である. 同じく, $z \in C_y$ だから, $y \equiv z$ である. そして $\equiv$ の推移性を使うと $x \equiv y$ を得る. □

商集合

定義 2.10. 集合 X 上に同値関係 $\equiv$ が設定されているとき, そこに現れる全ての同値類を集めて得られる集合

$$\bar{X} = \{C_x \mid x \in X\}$$

を X の同値関係 $\equiv$ による**商集合**と呼ぶ.

商集合 $\bar{X}$ の元 C_x は同値類であり, その実体は X の空でない部分集合である. よって, $\bar{X}$ **は** X **の部分集合から成る集合族**である.

全ての $x \in X$ についてそれが作る同値類 C_x を列挙したとき, x に応じて全て異なる同値類が出てくるとは限らない. 命題 2.9(2) から, $x \neq y$ であっても, $x \equiv y$ であれば $C_x = C_y$ となるので, 全ての x についてその同値類 C_x を列挙していくと, 重複して現れるものがたくさん出てくる可能性がある. 例えば, x と同値な元が n 個あれば, C_x が n 回現れることになる. 重複分は省いて, 各々の同値類を一つずつ集めて作られる集合族が商集合である. 任意の $x \in X$ に対して, x が属する同値類 C_x を対応づける写像

$$\pi : X \to \bar{X}, \quad x \mapsto C_x$$

は X から商集合 $\bar{X}$ への全射であり, これを**類別写像**と言う.[*3]

同値類分割

定理 2.11. 集合 X 上に同値関係 $\equiv$ が設定されているとき, X は $\equiv$ によって生じる全ての同値類たちの非交和である. この非交和分解を X の $\equiv$ による**同値類分割**と呼ぶ.

証明. 全ての同値類 $C \in \bar{X}$ に渡る和集合を $\tilde{X}$ とする. 命題 2.9(2), (3) から, 相異なる同値類どうしは交わらないので, $\tilde{X}$ は全ての同値類 C に渡る非交和である.

どの同値類 C も X の部分集合であるから, $X \supseteq \tilde{X}$ である. 任意の $x \in X$ について, 命題 2.9(1) から x はその同値類 $C_x \in \bar{X}$ に属するので, $x \in C_x \subseteq \tilde{X}$ でもある. ゆえに, $X \subseteq \tilde{X}$ でもあり, $X = \tilde{X}$ が成り立つ. □

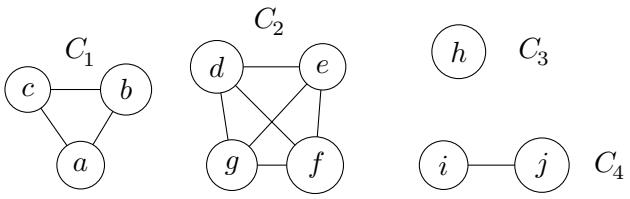


図 4　$X = \{a, b, c, \ldots, i, j\}$ が 4 つの同値類 C_1, C_2, C_3, C_4 に分割されたところ.

X の元を平面上に並べて, $x \equiv y$ となる 2 点 x, y を互いに全て辺で結ぶ. その結果, 図 4 のようになったとする. この図では, $X = \{a, b, c, \ldots, i, j\}$ が 4 つのグループ C_1, C_2, C_3, C_4 に分割されているが, その各々のグループが一つの同値類を形成している. X の商集合は $\bar{X} = \{C_1, C_2, C_3, C_4\}$ である. 図 4 のように, 異なる同値類の間には辺が一切存在せず, 同じ同値類に属する 2 点間には必ず辺が存在する. a と c は同じ類 C_1 に属するので $x \equiv y$ であり, $C_a = C_1 = C_c$ である. a と d は互いに異なる類に属しているということは, $a \neq d$ だということである. C_3 のように, 単独の点のみで一つの同値類をなしていることもある.

♦ **例 2.12**　とある学校にはいくつかのクラブがあって, 全ての生徒はそれぞれどれか 1 つのクラブに所属しているとする. ただし, 2 つ以上のクラブをかけもちすることはできないものとする. この学校の生徒の全体を X として, $x, y \in X$ に対して, $x \equiv y$ であることを「x と y は同じクラブに所属している」ことと定義する. $\equiv$ は X 上の同値関係であり, 生徒 x の同値類 C_x は x と同じクラブに所属している生徒の全体である. 例えば, x がサッカー部に所属しているなら, C_x はサッカー部員の全体である. x, y がどちらも同じクラブの部員であれば, たとえ $x \neq y$ であっても, $C_x = C_y$ である. X はいくつかの同値類に分かれるが, 各々の同値類は「野球部員の全体」「吹奏楽部員の全体」のように, 何らかのクラブの部員全体である. □

♦ **例 2.13**　例 2.4 で示した同値関係は, 組 (a, b) をそれが表す分数 a/b の値に応じて分類するものであった. よって, (a, b) の同値類 $C_{(a,b)}$ に属する全ての組 (a', b') は a/b と同じ分数を表している. このように, 一つの同値類 $C_{(a,b)}$ に対してそれ固有の分数 a/b が対応していると考えてよい. これは同値類が無限個出てくる一例である. □

[*3] **分類写像**, **標準全射**, **自然な全射**など, 別の言葉で呼ばれることも多い. ここでは, X の元を同値類へ分類するという意味を込めて「類別写像」と呼んでいる.

♦ **例 2.14**　例 2.2 の同値関係は $\mathbb{R}^2$ の点を原点からの直線距離に応じて分類する関係なので, 各々の同値類はある半径 $r \geq 0$ に対する円周 $C_r = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = r^2\}$ である. よって, $\mathbb{R}^2$ はこれらの円周の非交和として $\mathbb{R}^2 = \bigcup_{r \geq 0} C_r$ と分解される. これも同値類が無限個出てくる一例である. 図 5 にこ

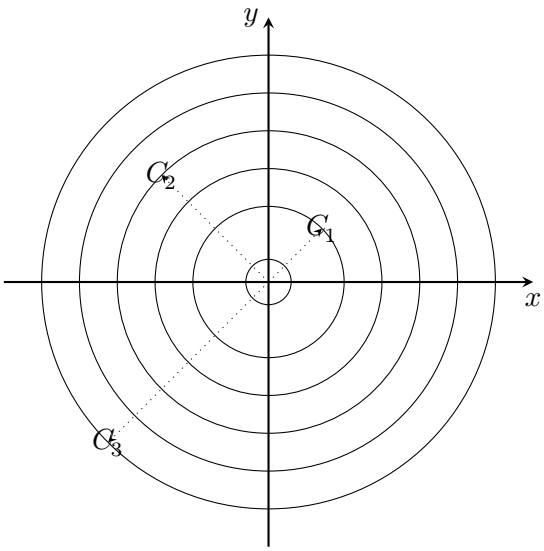


図 5　例 2.2 の同値関係で $\mathbb{R}^2$ を同値類分割したところ.

の同値類分割のイメージ図を描いた. 図中には明示されていないが, 原点はそれ一つで単独の同値類 C_0 を形成している. □

♦ **例 2.15**　$\mathbb{Z}$ 上で自然数 $n > 1$ を法とする合同関係 $\equiv$ (例 2.5) を考えよう:

$$x \equiv y \overset{\text{def}}{\iff} x - y \in n\mathbb{Z}.$$

任意の整数 x について, それが属する同値類を C_x とするとき, 次のことが成り立つことを示そう.

(1) 任意の整数 x について, $C_x = x + n\mathbb{Z}$ である. ここで, $x + n\mathbb{Z}$ は n の倍数と x との和で表される整数 $x + nk$ $(k \in \mathbb{Z})$ の全体を表している.
(2) 任意の整数 x について, それを n で割った時の余りを r とするとき, $C_x = C_r$ である.
(3) $r, r' \in \{0, 1, \ldots, n-1\}$ ならば, $r = r' \iff C_r = C_{r'}$ である. よって, $C_0, \ldots, C_{r-1}$ は全て異なる同値類である.
(4) $\mathbb{Z}$ の $\equiv$ による商集合 (それを $\mathbb{Z}/n\mathbb{Z}$ と書く) は次の式で与えられる:

$$\mathbb{Z}/n\mathbb{Z} = \{C_0, \ldots, C_{r-1}\} = \{r + n\mathbb{Z} \mid r = 0, 1, \ldots, n-1\}. \tag{4}$$

(1) $\equiv$ の定義から, 任意の $a \in \mathbb{Z}$ について, 次の同値が成立する:

$$a \in C_x \iff a \equiv x \iff a - x \in n\mathbb{Z} \iff a \in x + n\mathbb{Z}.$$

よって, $C_x = x + n\mathbb{Z}$ である.

(2) x を n で割った時の商と余りをそれぞれ q, r とすると, $x - r = nq \in n\mathbb{Z}$ だから, $x \equiv r$ である. したがって, 命題 2.9(2) から $C_x = C_r$ でもある.

(3) $0 \leq r, r' < n$, $C_r = C_{r'}$ とする. $r \equiv r'$ だから, $r - r'$ は n の倍数であるが, $0 \leq r, r' < n$ だから, $r - r' = 0$, つまり $r = r'$ である.

(4) (3) から $C_0, C_1, \dots, C_{n-1}$ は全て異なり, (2) からどの同値類 C_x もこの中のどれか一つと一致するので, 同値類は $C_0, C_1, \dots, C_{n-1}$ で全てである. ゆえに, 式 (4) が成立する. □

例えば $n = 4$ の場合には, $\mathbb{Z}$ は $n = 4$ を法とする合同関係により次の 4 個の同値類に分割される:

$$
\begin{aligned}
0 + 4\mathbb{Z} &= \{\dots, -12, -8, -4, 0, 4, 8, 12, \dots\}, \\
1 + 4\mathbb{Z} &= \{\dots, -11, -7, -3, 1, 5, 9, 13, \dots\}, \\
2 + 4\mathbb{Z} &= \{\dots, -10, -6, -2, 2, 6, 10, 14, \dots\}, \\
3 + 4\mathbb{Z} &= \{\dots, -9, -5, -1, 3, 7, 11, 15, \dots\}.
\end{aligned}
$$

見ての通り, $0 + 4\mathbb{Z} = 4\mathbb{Z}$ は 4 の倍数の全体であり, $1 + 4\mathbb{Z}$, $2 + 4\mathbb{Z}$, $3 + 4\mathbb{Z}$ はそれぞれ 4 で割ると 1, 2, 3 余る整数の全体である. 商集合 $\mathbb{Z}/4\mathbb{Z}$ はこれら 4 個の同値類から成る族である.

♦ **例 2.16**　例 2.7 をもう一度考えよう. $G = (V, E)$ を無向グラフとし, 2 点 $x, y \in V$ に対して $x \to y$ を「G 上に x から y に至る道が存在する」で定義すれば, $\to$ は V 上の同値関係であるという話だった. この関係 $\to$ を図 6 に描かれたグラフ G 上で考えてみよう. 図の通り, このグラフ G は 2 つの '島' G_1, G_2 で構成されていて, G_1 と G_2 の間には '橋' がかかっていない. 点集合 $V = \{x_1, x_2, \dots, x_9\}$ を同値関係 $\to$ で同値類分割すると, 2 つの同値類 $V_1 = \{x_1, x_2, \dots, x_6\}$ と $V_2 = \{x_7, x_8, x_9\}$ が生じるが, V_1 上の点どうしを結ぶ辺のみで構成される部分グラフが G_1 であり, V_2 上の点どうしを結ぶ辺のみで構成される部分グラフが G_2 であり, G はこの 2 つの部分グラフ (それぞれ G の**連結成分**と呼ばれる) で構成される. □

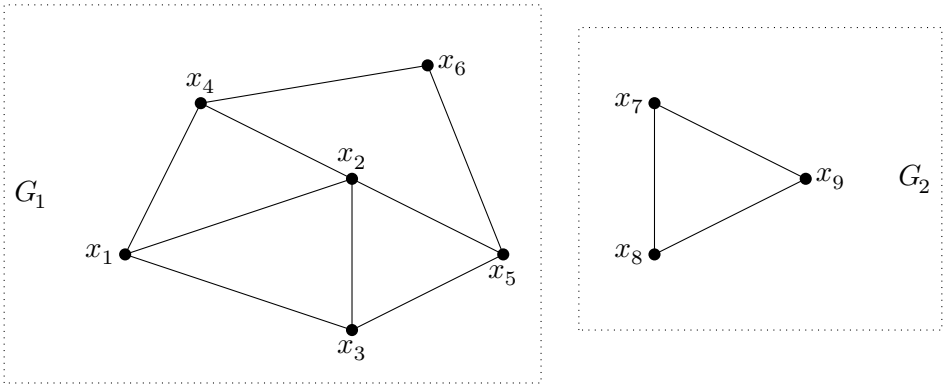


図 6　非連結な無向グラフの例.

ここまでに, 同値関係は集合を分割するという事例をいくつか見てきた. それとは逆に, 集合 X の任意の分割は X 上に同値関係を定めることも言える. $X = \bigcup_{i \in I} X_i$ が X の分割であるとき, $x, y \in X$ に対して, $x \equiv y$ であることを「x, y は同一の X_i に属している」ことと定義する. $\{X_i\}_{i \in I}$ が X の分割をなすことから, $\equiv$ が同値関係であることはすぐわかる. そして, 各々の X_i は $\equiv$ に関する同値類を形成している. このように, **集合 X 上に同値関係を定めることと, X を分割することは本質的には同じ効果を持っている**.

2.3　完全代表系

X に現れる各同値類 $C \in \bar{X}$ から任意に一つずつ元 x_C を選び, それらの元の全体を $P = \{x_C\}_{C \in \bar{X}}$ とする. このように, 各々の同値類から元を一つずつ集めて得られる集合 P を X の**完全代表系**と言い, 同値

類 C から選ばれた元 x_C は C の**代表元**と呼ばれる (図 7). 言い換えれば, 完全代表系とは次の 2 条件を満たす部分集合 $P \subseteq X$ のことである:

(1) 任意の $x \in X$ に応じて, $x \equiv p$ となる元 $p \in P$ が必ず存在する. つまり, p は同値類 C_x の代表元である.
(2) $p, p' \in P$ を相異なる元とするとき, $p \not\equiv p'$ である. つまり, 一つの同値類から選ばれる代表元は 1 つだけである.

これらの条件は, 類別写像 $\pi : X \to \bar{X}$ の始集合を P に制限した写像 $\pi|_P : P \to \bar{X}$ が全単射であるということと同じ意味である.

P を完全代表系とする. $p \in P$ のとき, それが同値類 C から選ばれた代表元であるとすると, $C = C_p$ である. よって,

$$X = \bigcup_{C \in \bar{X}} C = \bigcup_{p \in P} C_p$$

である. これが X の同値類分割になっている.

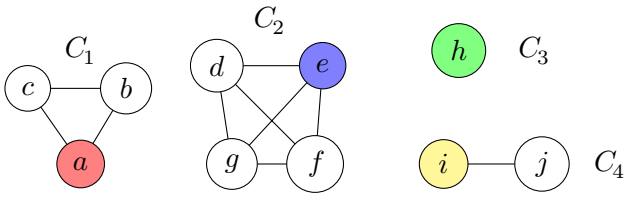


図 7　完全代表系 $\{a, e, h, i\}$ の作り方 (図 4 と同じ図を使用). それぞれ, 色付きの元が代表元.

完全代表系 P の作り方は一意的ではない. 各同値類からどの代表元を選んでくるかで P は変わるからである. 例えば, 図 7 の場合, 完全代表系は全部で $|C_1| \times |C_2| \times |C_3| \times |C_4| = 24$ 通りある.

♦ **例 2.17**　例 2.12 についてもう一度考えると, X 上の完全代表系とは, 各々のクラブから一人の部員をそのクラブの代表者として集めてきてできる集合である. 各クラブの代表者はちょうど 1 名であり, 0 名であっても, 2 名以上であってもいけない. どのクラブからどの代表者を選出するかによって, 完全代表系の作り方はたくさんあり得る. □

♦ **例 2.18**　$\mathbb{Z}$ 上で $n = 4$ を法とする合同関係を考えるとき, $P = \{0, 1, 2, 3\}$ は完全代表系の一つである. 一方で, $P' = \{1, 2, 3, 4\}$ も完全代表系である. 4 と 0 は合同だから, 同値類 $C_0 = 4\mathbb{Z}$ の代表元として 0 の代わりに 4 を選んでもいいからである. さらに, $P'' = \{16, 5, -2, 7\}$ も完全代表系である. これは, それぞれ $16 \equiv 0$, $5 \equiv 1$, $-2 \equiv 2$, $7 \equiv 3$ であることによる. このように, 完全代表系の作り方は無数にあるが, 普通は最もわかりやすい $\{0, 1, 2, 3\}$ または $\{1, 2, 3, 4\}$ あたりを考える. □

面倒くさいことを言えば, X 上に同値類が無限個現れる場合には, 完全代表系を得るには選択公理が必要になる可能性がある. (可能性があるだけで, いつでも必要というわけではない.) 同値類が無限個ある場合に完全代表系を作る操作は, 空でない無限個の集合らに渡る選択集合を作る操作に当からである.

▶ **演習 2.4**　(この演習問題は線型代数学の知識がある読者向け) 演習 2.1 で述べた同値関係 $\equiv$ を考える.

(1) 任意の $A, B \in \mathrm{GL}_n(\mathbb{R})$ について, $A \equiv B \iff \det A = \det B$ であることを示せ. ($\det$ は行列式を表している.)
(2) $\mathrm{GL}_n(\mathbb{R})$ を同値類分割したときの完全代表系を具体的に一つ与えよ.

▶ **演習 2.5**　$\mathcal{P}$ を $\mathbb{Z}$ の全ての有限部分集合から成る集合族とし, この上の関係 $\equiv$ を次の式で定める: 任意の $A, B \in \mathcal{P}$ について,

$$A \equiv B \overset{\text{def}}{\iff} A \vartriangle B \text{ が偶数個の元から成る.}$$

$\equiv$ は同値関係であることを示し, $\mathcal{P}$ をそれで同値類分割したときの完全代表系を具体的に一つ与えよ.

▶ **演習 2.6**　$\mathbb{C}$ 上の関係 $\equiv$ を次の式で定める: $w, z \in \mathbb{C}$ に対して,

$$w \equiv z \overset{\text{def}}{\iff} w - z \text{ は格子点である.}$$

ここで**格子点**とは, 実部と虚部がともに整数である複素数のことである.

(1) $\equiv$ は同値関係であることを示せ.
(2) $\mathbb{C}$ を同値類分割したとき,

$$I = \{a + bi \mid a, b \in [0, 1)\}$$

は完全代表系であることを示せ. ここで, $[0, 1) = \{x \in \mathbb{R} \mid 0 \leq x < 1\}$ である.

2.4　商写像

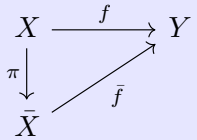
$f : X \to Y$ を写像とし, 始集合 X 上に同値関係 $\equiv$ が設定されているとする. f が**同値関係 $\equiv$ を保つ**とは, 任意の $x, x' \in X$ に対して次の条件式が成り立つことを言う:

$$x \equiv x' \Rightarrow f(x) = f(x').$$

図 8 は X 上の同値関係 $\equiv$ を保っている写像 f と保っていない写像 g のイメージを描いている. g では, 赤線で示された 2 つの元は同じ同値類 C_3 に属していながら互いに異なる元 a, b に変換されている. 一方で, f ではそのようなことは起こっておらず, 同じ同値類に属する元は全て同一の元に変換されている. この f のように同値関係 $\equiv$ を保つ写像では, 各同値類 C について, それに属する元は全て同じ元 y に変換されるので, f は同値類 C をその元 y に変換していると見なすこともできる.

商写像

命題 2.19. $f : X \to Y$ を写像とし, 始集合 X 上に同値関係 $\equiv$ が設定されているとする. このとき, f が $\equiv$ を保つためには, 写像 $\bar{f} : \bar{X} \to Y$ で $\bar{f} \circ \pi = f$ となるものが存在することが必要十分である:



ただし, $\bar{X}$ は X の同値関係 $\equiv$ による商集合であり, $\pi : X \to \bar{X}$ は類別写像である.

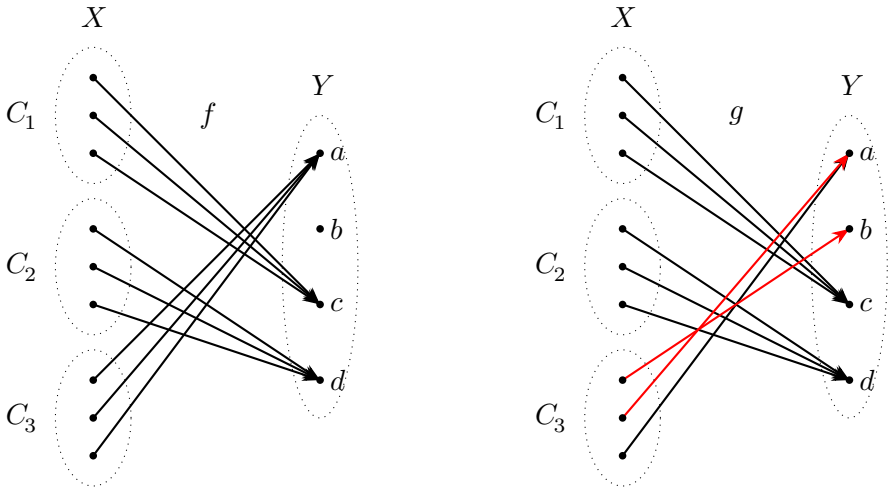


図 8　同値関係を保つ写像 f と保っていない写像 g.

証明. f が $\equiv$ を保つと仮定する. $\bar{X}$ は X 上に生じる同値類から成る集合族であるから, その任意の元 C は, それに属する代表元 x を任意に選んで $C = \pi(x)$ (x が属する同値類) という形式で記述される. これを用いて, 写像 $\bar{f} : \bar{X} \to Y$ を次の式で定義することを考える:

$$\bar{f} : \bar{X} \to Y, \quad C \mapsto f(x), \quad \text{ただし } C = \pi(x)\ (x \in X). \tag{5}$$

一般には, 同一の同値類 C に対して複数の代表元による表示が可能である. すなわち, $x, x' \in X$ に対して, たとえ $x \neq x'$ であったとしても, それらが表す同値類 $\pi(x)$, $\pi(x')$ はどちらも同じ同値類 C であるということがあり得る. このように, $\pi(x) = C = \pi(x')$ ならば $x \equiv x'$ であるから, f が $\equiv$ を保つことから $f(x) = f(x')$ となる. すなわち, 最終的に得られる $\bar{f}(C)$ の値は, C を表すために用いられる代表元 x をどのように選んでも, 結局は C に応じて一意的に決まる値である. このことから, 式 (5) によって $\bar{f}$ は $\bar{X}$ から Y への単価写像として正しく定まっていることが分かる. 式 (5) から, 任意の $x \in X$ について $\bar{f}(\pi(x)) = f(x)$ であるから, $\bar{f} \circ \pi = f$ となる.

次は逆に, $\bar{f} \circ \pi = f$ となる写像 $\bar{f} : \bar{X} \to Y$ が存在すると仮定する. $x, x' \in X$, $x \equiv x'$ であるとすると, $\pi(x) = \pi(x')$ なので, 仮定から $f(x) = \bar{f} \circ \pi(x) = \bar{f} \circ \pi(x') = f(x')$ となる. ゆえに, f は $\equiv$ を保つ. □

$f : X \to Y$ が X 上の同値関係 $\equiv$ を保つとき, この命題から, $\bar{f} \circ \pi = f$ となる写像 $\bar{f} : \bar{X} \to Y$ が存在する. ここで, π は商集合 $\bar{X}$ の上への全射なので, 第 2 巻『写像』命題 4.6(2) を利用すれば, この条件 $\bar{f} \circ \pi = f$ を満たす写像 $\bar{f}$ は唯一つに決まることがわかる. この写像 $\bar{f}$ を f の同値関係 $\equiv$ による**商写像**と言う. 例えば, 図 8 の写像 f の場合, X の商集合は $\bar{X} = \{C_1, C_2, C_3\}$ であり, f の商写像 $\bar{f}$ は $\bar{f}(C_1) = c$, $\bar{f}(C_2) = d$, $\bar{f}(C_3) = a$ で定まる写像である.

f が同値関係 $\equiv$ を保たないとき, 次の通り商写像 $\bar{f}$ は多価写像になる. f は $\equiv$ を保たないので, $x \equiv x'$ であるが $f(x) \neq f(x')$ となる $x, x' \in X$ が存在する. $x \equiv x'$ だから同値類としては $\pi(x) = \pi(x')$ であり, この同値類を C で表すことにすると, $\bar{f}$ の定義から,

$$\bar{f}(C) = \bar{f} \circ \pi(x) = f(x),$$
$$\bar{f}(C) = \bar{f} \circ \pi(x') = f(x')$$

☕ Coffee Break ☕

商写像と well-defined

写像 $f : X \to Y$ の商写像 $\bar{f} : \bar{X} \to Y$ は同値類 $C = \pi(x)$ に $f(x)$ を対応づける写像である．f は X の元を入力として受け取るが，それに対して $\bar{f}$ は X の個々の元ではなく，同値類を入力として受け取るという違いがある．

ここで重要なポイントは，**$\bar{f}(C)$ の値は見かけ上 C の代表元 x を用いて記述されているが，実際には C の中からどの x を代表として選んでも，それには関係なく $\bar{f}(C)$ の値は C から一意的に決まる**ということである．(そのための条件が，f が $\equiv$ を保つということである.) このような状況を指して，$\bar{f}$ は**うまく定義されている**と言ったり，あるいは日本語に訳さず英語のまま **well-defined** であると言ったりする．このように，定義が well-defined かどうかを気にする必要があるのは，同一の同値類を代表元を用いて記述する方法が複数通りあり得るからである．

となる．このように，$\bar{f}(C)$ の値が複数個現れることになる．例えば，図 8 の写像 g から無理やり商写像 $\bar{g}$ を作ると，$\bar{g}(C_3)$ の値として a と b が現れることになる．

♦ **例 2.20**　G を実数成分の n 次正則行列の全体とする．任意の行列 $A, B \in G$ に対して，

$$A \equiv B \overset{\text{def}}{\iff} P^{-1}AP = B \text{ となる } P \in G \text{ が存在する}$$

と定義する．この関係 $\equiv$ は G 上の同値関係である．(これは線型代数学で行列の**相似**と呼ばれる関係である.) この同値関係による G の商集合を $\bar{G}$ で表す．

写像 $f : G \to \mathbb{R}$ を行列式写像とする．すなわち，$f(A) = \det A$ (A の行列式) とする．一般に，$A, B \in G$, $A \equiv B$ ならば，ある $P \in G$ に対して $P^{-1}AP = B$ と書けるので，

$$f(B) = f(P^{-1}AP) = \det(P^{-1}AP) = (\det P)^{-1}(\det A)(\det P) = \det A = f(A)$$

となる．したがって，f は $\equiv$ を保つ．よって，f の商写像 $\bar{f} : \bar{G} \to \mathbb{R}$ が定義される．行列 $A \in G$ の同値類を $\bar{A} \in \bar{G}$ で表すことにすると，$\bar{f}(\bar{A}) = f(A) = \det A$ である．商写像 $\bar{f}$ が一つの単価写像として正しく定まるのは，どの同値類についても，それに属する行列が全て同じ行列式を持っているからである．すなわち，本来は個々の正方行列に対して定義されている行列式という値を**各々の相似類に対して定義されている値と見なすことができる**ということである．

一方，写像 $g : G \to \mathbb{R}$ を次の式で定める:

$$g(A) \overset{\text{def}}{=} A \text{ の全ての成分の合計値.}$$

例えば，行列 $A, B \in G$ を

$$A = \begin{pmatrix} 2 & 1 \\ -1 & 3 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 2 \\ 0 & -1 \end{pmatrix}^{-1} A \begin{pmatrix} 1 & 2 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 4 & 13 \\ 1 & 5 \end{pmatrix}$$

とおくと，$A \equiv B$ ではあるが，$g(A) = 5$, $g(B) = 23$ なので，$g(A) \neq g(B)$ である．よって，g は $\equiv$ を保っていない．このような状況で g の商写像 $\bar{g}$ を無理やり考えると多価写像が出てくる．上記の A, B に対して $A \equiv B$ なので，同値類 $\bar{A}$, $\bar{B}$ は見かけは違えどもどちらも同じ同値類である．その同値類を C で表すと，$\bar{g}(C) = \bar{g}(\bar{A}) = g(A) = 5$, $\bar{g}(C) = \bar{g}(\bar{B}) = g(B) = 23$ となって，$\bar{g}(C)$ の値が複数になってしまう．　□

▶ **演習 2.7**　$f : X \to Y$ を写像とする．X 上に同値関係 $\equiv$ が設定されていて，f は $\equiv$ を保っているとする．f の商写像を $\bar{f} : \bar{X} \to Y$ で表す．このとき，次のことを証明せよ．

(1) $\bar{f}$ が単射であるためには，任意の $x, x' \in X$ に対して次の条件式が成り立つことが必要十分である:

$$x \equiv x' \iff f(x) = f(x').$$

(2) $\bar{f}$ が全射であるためには，f が全射であることが必要十分である．

▶ **演習 2.8**　任意の写像 $f : X \to Y$ は全射 $u : X \to Z$ と単射 $v : Z \to Y$ の合成 $f = v \circ u$ で表されることを示せ．(Hint: X 上で同値関係 $x \equiv x' \overset{\text{def}}{\iff} f(x) = f(x')$ を考えて，これによる X の商集合を Z とする.)

3　おまけ: 初等整数論への応用

この節は同値関係の応用事例として初等整数論に関する話題を提供することが目的である．この節全体が一つの大きな例のようなものだから，全部を省略しても全く差し支えない．

3.1　剰余環 $\mathbb{Z}/n\mathbb{Z}$

以下，n を 2 以上の自然数とする．

例 2.5 で述べた，$\mathbb{Z}$ における n を法とする合同関係を考えよう．これは，

$$a \equiv b \pmod{n} \overset{\text{def}}{\iff} a - b \in n\mathbb{Z}$$

で定まる同値関係 $\equiv$ である．ここで，$n\mathbb{Z}$ は n の倍数の全体集合である．以下，n が文脈から明らかである場合には $(\mathrm{mod}\ n)$ の記述は省略する．

n を法とする合同関係 $\equiv$ による $\mathbb{Z}$ の商集合を $\mathbb{Z}/n\mathbb{Z}$ と書き，$\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ を分類写像とする．つまり，整数 a に対して $\pi(a)$ は a を含む同値類であるが，具体的に書けば

$$\pi(a) = a + n\mathbb{Z} = \{a + nk \mid k \in \mathbb{Z}\}$$

であり，これは a と n の倍数との和で表される整数の全体である．これを，n を法とする整数 a の**剰余類**と呼ぶ．$\mathbb{Z}/n\mathbb{Z}$ はこれら全ての剰余類 $\pi(a)$ の集まりである:

$$\mathbb{Z}/n\mathbb{Z} = \{\pi(a) \mid a \in \mathbb{Z}\}.$$

a が整数全体を動くごとにそれぞれ相異なる同値類 $\pi(a)$ が現れるというわけではなく，整数 a, a' が $a \equiv a'$ を満たしているとき，かつその時に限り $\pi(a) = \pi(a')$ である．a を n で割った時の余りを r とすると $\pi(a) = \pi(r)$ となるので，どの剰余類もそれぞれ $\pi(0), \pi(1), \ldots, \pi(n-1)$ のうちのいずれか一つと一致する．よって，

$$\mathbb{Z}/n\mathbb{Z} = \{\pi(r) \mid r = 0, 1, 2, \ldots, n-1\}$$

である．ここに挙げられた n 個の剰余類は全て異なっているので，$\mathbb{Z}/n\mathbb{Z}$ はちょうど n 個の剰余類から成る有限集合である．

可換環　さて, ご存知の通り $\mathbb{Z}$ 上には加法 (和) および乗法 (積) という 2 つの演算が備わっている. それらは, よく知られている通り次の基本的な規則を満たしている. 以下, a, b, c は任意の整数を表している.

(1) **加法に関する基本規則**
　結合則: $a+(b+c)=(a+b)+c$.
　可換則: $a+b=b+a$.
　零元則: $a+0=0+a=a$.
　負元則: $a+(-a)=(-a)+a=0$. (補足: $-a$ の立場から見れば, その負元は $-(-a)=a$ である.)

(2) **乗法に関する基本規則**
　結合則: $a(bc)=(ab)c$.
　可換則: $ab=ba$.
　単位則: $a\times 1=1\times a=a$.

(3) **加法と乗法の両方に関する基本規則**
　分配則: $a(b+c)=ab+ac$. (これと積の交換則から, $(b+c)a=a(b+c)=ab+ac=ba+ca$ も成り立つ.)

$\mathbb{Z}$ の加法と乗法がこれらの規則を満たしていることを指して, 抽象代数学の用語で $\mathbb{Z}$ はその加法と乗法に関して**可換環**[*4]であると言う. (可換環とは, 加法と乗法を備えた空でない集合であって, 上で述べた 8 個の規則を全て満たしているものを言う. なお, 単に**環**と言う場合には, 乗法の可換則 $xy=yx$ は必ずしも前提とされないが, 以下では簡単のためもっぱら可換環のみを考える.) $\mathbb{Z}$ だけでなく, $\mathbb{Q}$, $\mathbb{R}$ および $\mathbb{C}$ もそれぞれの加法と乗法について可換環である.

「0 には何を掛けても 0」という事実はよく知られているが, これはあらゆる可換環で通用する. R を任意の可換環とするとき, まず零元則から $0=0+0$ なので,[*5] 任意の $a\in R$ について分配則を適用すれば $a\times 0=a(0+0)=a\times 0+a\times 0$ となる. ここで, 負元則から $-(a\times 0)$ が存在するが, それを両辺に加えれば

$$a\times 0+(-(a\times 0))=(a\times 0+a\times 0)+(-(a\times 0))$$

となる. この左辺は 0 である. 一方, 右辺は結合則を使えば $a\times 0+(a\times 0+(-a\times 0))=a\times 0+0$ となるが, さらに零元則からこれは $a\times 0$ である. よって, $a\times 0=0$ である. 交換則から, $0\times a=0$ であることも言える. このように, どんな可換環でも 0 との積は常に 0 であるが, このことを使えば, 任意の元 $x\in R$ について

$$0=0\times x=(1+(-1))x=1\times x+(-1)x=x+(-1)x$$

であり,[*6] ここから

$$(-1)x=-x$$

であることが言える. これはつまり,「-1 倍すると符号が反転する」という周知の規則があらゆる可換環で通用することを示している. これを特に $x=-1$ に対して適用すれば, $(-1)^2=-(-1)=1$ が得られる.[*7]

[*4]「かかんかん」と読む. 英語では commutative ring.
[*5] 細かいことだが, ここで言う 0 は整数としての 0 ではなくて, R において加法について零の役目を果たす元 (零元) のことである.
[*6] ここでも, 1 は整数としての 1 ではなくて, R において乗法について単位元として働く元のことである.
[*7] この事実が「負の数どうしの積は正である」という周知の事実を正当化する.

剰余環 $\mathbb{Z}/n\mathbb{Z}$　ここで, 話を商集合 $\mathbb{Z}/n\mathbb{Z}$ に戻そう. $\mathbb{Z}/n\mathbb{Z}$ の各々の元は何らかの整数 a の剰余類 $\pi(a)$ である. そこで, 任意の整数 $a, b \in \mathbb{Z}$ に対して,

$$\begin{aligned} \pi(a) \oplus \pi(b) &\stackrel{\text{def}}{=} \pi(a+b), \\ \pi(a) \otimes \pi(b) &\stackrel{\text{def}}{=} \pi(ab) \end{aligned} \tag{6}$$

と定義することで, 商集合 $\mathbb{Z}/n\mathbb{Z}$ 上にもそれぞれ加法 $\oplus$ と乗法 $\otimes$ が定義される.[*8] これらは剰余類どうしの和と積を定める規則であり, 演算結果もまた一つの剰余類であるところに注意しておこう.

ところで, 式 (6) は一見自然で分かりやすい定義であるが, これには要注意である. と言うのも, 2.4 節でも述べたことだが, **剰余類には表現の多様性がある**からである. つまり, 整数 a, a' が相異なる整数であっても, $a \equiv a'$ でさえあれば, 剰余類としては $\pi(a) = \pi(a')$ であり,「a の剰余類」と呼んでも「a' の剰余類」と呼んでも実は同じ剰余類を指している. 式 (6) に定義された加法と乗法が, この剰余類表現の多様性にきっちり対応できているかが問題である. $\pi(a) = \pi(a')$ かつ $\pi(b) = \pi(b')$ であるとき, 和 $\oplus$ の定義によれば

$$\begin{aligned} \pi(a) \oplus \pi(b) &= \pi(a+b), \\ \pi(a') \oplus \pi(b') &= \pi(a'+b') \end{aligned}$$

となるが, $\pi(a) = \pi(a')$ かつ $\pi(b) = \pi(b')$ だから, この 2 つの式は見かけは違えども同じ式である. なので, $\pi(a+b)$ と $\pi(a'+b')$ も (見かけは違うが) 同一の剰余類でなければ不都合である. そうでないと, 同一の和 $\pi(a) \oplus \pi(b) = \pi(a') \oplus \pi(b')$ が複数の異なる結果を持ち得ることになってしまうからである. 積 $\otimes$ についても同様である.

格言: 同値類に対して何かを定義するときには, 同値類表現の多様性に注意!

さて, 式 (6) の定義が剰余類表現の多様性にうまく対応できていることを確かめるには, $\pi(a) = \pi(a')$ かつ $\pi(b) = \pi(b')$ であれば必ず $\pi(a+b) = \pi(a'+b')$ かつ $\pi(ab) = \pi(a'b')$ であることを確かめればよい. $\pi(a) = \pi(a')$ かつ $\pi(b) = \pi(b')$ なので, $a \equiv a'$ かつ $b \equiv b'$ であり, したがってそれぞれある整数 $k, l \in \mathbb{Z}$ を用いて

$$a - a' = nk, \quad b - b' = nl$$

と書ける. すると,

$$\begin{aligned} a + b - (a' + b') &= (a - a') + (b - b') = n(k + l) \in n\mathbb{Z}, \\ ab - a'b' &= ab - a'b + a'b - a'b' \\ &= (a - a')y + a'(b - b') \\ &= n(ky + x'l) \in n\mathbb{Z} \end{aligned}$$

となるので, $a + b \equiv a' + b'$ かつ $ab \equiv a'b'$, すなわち $\pi(a+b) = \pi(a'+b')$ かつ $\pi(ab) = \pi(a'b')$ である. これでようやく, 式 (6) によって $\mathbb{Z}/n\mathbb{Z}$ 上の加法 $\otimes$ と乗法 $\otimes$ が問題なく定義できることが分かった.

$\mathbb{Z}/n\mathbb{Z}$ における加法 $\oplus$ と乗法 $\otimes$ の定義から容易に分かることだが, これらは $\mathbb{Z}$ における加法と乗法の基本規則——可換環としての規則——を色濃く受け継いでいる.

(1) **加法に関する基本規則**

[*8] これは一つの**定義**であって, $\pi(a)$ と $\pi(b)$ の和が $\pi(a+b)$ になるという '定理' ではない. 積についてももちろん同じ.

結合則: $\pi(a) \oplus (\pi(b) \oplus \pi(c)) = (\pi(a) \oplus \pi(b)) \oplus \pi(c)$.
可換則: $\pi(a) \oplus \pi(b) = \pi(b) \oplus \pi(a)$.
零元則: $\pi(a) \oplus \pi(0) = \pi(0) \oplus \pi(a) = \pi(a)$.
負元則: $\pi(a) \oplus \pi(-a) = \pi(-a) \oplus \pi(a) = \pi(0)$. (つまり, $\pi(-a) = -\pi(a)$ ということ.)

(2) **乗法に関する基本規則**
結合則: $\pi(a) \otimes (\pi(b) \otimes \pi(c)) = (\pi(a) \otimes \pi(b)) \otimes \pi(c)$.
可換則: $\pi(a) \otimes \pi(b) = \pi(b) \otimes \pi(a)$.
単位則: $\pi(a) \otimes \pi(1) = \pi(1) \otimes \pi(a) = \pi(a)$.

(3) **加法と乗法の両方に関する基本規則**
分配則: $\pi(a) \otimes (\pi(b) \oplus \pi(c)) = \pi(a) \otimes \pi(b) \oplus \pi(a) \otimes \pi(c)$.

このように, 各々の整数 a を剰余類 $\pi(a)$ に置き換え, $+$ と $\times$ をそれぞれ $\oplus, \otimes$ で置き換えると, $\mathbb{Z}$ における可換環のルールがそっくりそのまま $\mathbb{Z}/n\mathbb{Z}$ 上でも成り立っていることが分かる. つまり, $\mathbb{Z}/n\mathbb{Z}$ もまた加法 $\oplus$ と乗法 $\otimes$ について一つの可換環になっている. これを n を法とする $\mathbb{Z}$ の**剰余環**と呼ぶ.

これ以後は, 剰余環 $\mathbb{Z}/n\mathbb{Z}$ における加法 $\oplus$ と乗法 $\otimes$ のこともそれぞれ通常の加法記号 $+$ と乗法記号 $\times$ で表すことにする. (慣例的に, 乗法記号 $\times$ は誤解の恐れがなければしばしば省略される.)

♦ **例 3.1**　$n = 6$ の場合を考える. $\mathbb{Z}/6\mathbb{Z}$ は 6 個の剰余類 $\pi(0), \pi(1), \pi(2), \pi(3), \pi(4), \pi(5)$ から成る集合である. そして, 例えば

$$\pi(2) + \pi(5) = \pi(7) = \pi(1),$$
$$\pi(2)\pi(5) = \pi(10) = \pi(4)$$

が成り立つ. $\pi(2), \pi(3) \neq 0$ であるが, $\pi(2)\pi(3) = \pi(6) = \pi(0)$ である. このように, $\mathbb{Z}/6\mathbb{Z}$ 上では 0 でない元どうしの積が 0 になり得る. これは $\mathbb{Z}$ では決して起こり得ない現象である. □

3.2　剰余環における可逆元

一般に, 任意の可換環 R において, $xy = yx = 1$ を満たす関係にある元 $x, y \in R$ は互いに他方の**逆元**であると言い,

$$x = y^{-1}, \quad y = x^{-1}$$

と書く. このように, 逆元を持つ元は**可逆**であると言う. 例えば, 単位元 1 は自分自身を逆元に持つ可逆元であるし, $(-1)^2 = 1$ なので, -1 も自分自身を逆元に持つ可逆元である. なお, 0 に何を掛けても 0 であり, 1 にはならないので, 0 は可逆ではない.[*9]

R における可逆な元の全体を R^* で表す. x が可逆であれば, その逆元 x^{-1} は x を逆元に持つ可逆元である. だから, $x \in R^*$ であれば常に $x^{-1} \in R^*$ でもある. $x, y \in R^*$ であるとき, 乗法の結合則を使えば

$$(xy)(y^{-1}x^{-1}) = x(yy^{-1})x^{-1} = xx^{-1} = 1$$

が得られるので, xy は $y^{-1}x^{-1}$ を逆数に持つ可逆元であり, $xy \in R^*$ が成り立つ. このように, R^* は逆元を取る操作と積を取る操作で共に閉じている. このことを指して, 抽象代数学の言葉で R^* は**群**であると言

[*9] 細かいことを言えば, 形式的には可換環の中には $0 = 1$ であるもの, つまり零元と単位元が同一であるものもあり得るが, ここではそのようなものは考えていない.

う.[*10] R^* のことを R の**単数群**と呼ぶ.

$\mathbb{Z}$ 上では可逆な元は 1 と -1 の 2 つだけなので, $\mathbb{Z}^* = \{1, -1\}$ である. (2 にも 1/2 という逆元があるじゃないかと思うかも知れないが, 1/2 は有理数ではあるが整数ではないので, $\mathbb{Z}$ における 2 の逆元とは言えない.) ところが, 剰余環 $\mathbb{Z}/n\mathbb{Z}$ では $\pi(1)$ と $-\pi(1) = \pi(n-1)$ 以外にも可逆なものが存在し得る.

♦ **例 3.2**　$n = 7$ の場合を考える. $\mathbb{Z}/7\mathbb{Z}$ は 7 個の剰余類 $\pi(0), \pi(1), \ldots, \pi(6)$ から成る集合である. そして,

$$\pi(1)\pi(1) = \pi(1), \quad \pi(2)\pi(4) = \pi(8) = \pi(1),$$
$$\pi(3)\pi(5) = \pi(15) = \pi(1), \quad \pi(6)\pi(6) = \pi(36) = \pi(1)$$

となるので, $\pi(0)$ 以外の 6 つの元は全て可逆である. つまり, 単数群 $(\mathbb{Z}/7\mathbb{Z})^*$ は $\pi(0)$ 以外の 6 つの剰余類から成る. □

この例で見たように, $\mathbb{Z}/7\mathbb{Z}$ では零元 $\pi(0)$ 以外の全ての元が可逆であるが, このように 0 以外の全ての元が可逆である可換環を抽象代数学の用語で**体** (たい) と呼ぶ. $\mathbb{Z}$ は体ではないが, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ は全て体である.

剰余環 $\mathbb{Z}/n\mathbb{Z}$ においてどの剰余類が可逆でどの剰余類が可逆でないかは, もちろん n の値によって事情が変わる. $\mathbb{Z}/n\mathbb{Z}$ における可逆元を調べるためには, 次の定理が基本的である. この定理は第 4 巻『順序関係』例 3.9 で示されているので, 証明はそちらをチェックしてほしい.

Bézout の等式

定理 3.3. $a, b \in \mathbb{Z}$ を整数, $d = \gcd(a, b)$ をそれらの最大公約数とするとき,

$$ax + by = d$$

を満たす整数 x, y が存在する.

ここでは, この定理を認めたうえで, それを利用して次の重要な定理を示す.

剰余環 $\mathbb{Z}/n\mathbb{Z}$ の可逆元

定理 3.4. $n \geq 2$ を自然数, a を整数とするとき, 剰余類 $\pi(a) = a + n\mathbb{Z}$ が剰余環 $\mathbb{Z}/n\mathbb{Z}$ において可逆であるためには, $\gcd(a, n) = 1$ であることが必要十分である.

証明. $\pi(a)$ が可逆であると仮定して, その逆元を $\pi(x)$ とすると, $\pi(ax) = \pi(a)\pi(x) = \pi(1)$, すなわち $ax \equiv 1$ なので, $ax - 1 \in n\mathbb{Z}$ である. そこで, ある整数 y を用いて $ax - 1 = ny$, つまり $ax - ny = 1$ と書ける. $d = \gcd(a, n)$ とおくと, ax, ny は共に d の倍数なので $1 = ax - ny$ も d の倍数であり, したがって $d = 1$ である.

逆に, $\gcd(a, n) = 1$ とすると, 定理 3.3 から $ax + ny = 1$ を満たす整数 a, x が存在する. $ax - 1 = -ny \in n\mathbb{Z}$ だから $ax \equiv 1$ であり, したがって $\pi(a)\pi(x) = \pi(ax) = \pi(1)$ である. ゆえに, $\pi(x)$ は $\pi(a)$ の逆元である. □

[*10] 群とは, 1 つの演算を持つ空でない集合で, 結合則, 単位則および逆元則を満たすものを言う.

系 3.5. $n \geq 2$ を自然数とするとき, 剰余環 $\mathbb{Z}/n\mathbb{Z}$ が体であるためには, n が素数であることが必要十分である.

証明. n が素数ならば, 0 から $n-1$ までの整数のうちで 0 を除く全ての整数 a は n と互いに素であり, 定理 3.4 からそれが定める剰余類 $\pi(a) = a + n\mathbb{Z}$ は $\mathbb{Z}/n\mathbb{Z}$ の可逆元である. よって, $\mathbb{Z}/n\mathbb{Z}$ では 0 を除く全ての元が可逆であり, $\mathbb{Z}/n\mathbb{Z}$ は体である. 逆に, $\mathbb{Z}/n\mathbb{Z}$ が体であれば, どの整数 a $(1 \leq a \leq n-1)$ についても剰余類 $\pi(a)$ は可逆であり, したがって定理 3.4 から $\gcd(a, n) = 1$ であるが, これは n が素数であることを意味する. □

3.3 Euler の定理

引き続き, $n \geq 2$ を自然数とする. 定理 3.4 から, $\mathbb{Z}/n\mathbb{Z}$ の単数群は

$$(\mathbb{Z}/n\mathbb{Z})^* = \{\pi(a) \mid \gcd(a, n) = 1\}$$

である. ここで, $\pi(a) = a + n\mathbb{Z}$ は a の剰余類を表している. 剰余類の代表元としては 0 から $n-1$ までの整数を考えておけば十分なので,

$$(\mathbb{Z}/n\mathbb{Z})^* = \{\pi(a) \mid 0 \leq a < n,\ \gcd(a, n) = 1\}$$

と書いてもよい. この単数群の大きさ (元の個数) のことを $\varphi(n)$ で表す. この関数 φ は初等整数論における基本的な関数の一つであり, Leonhard Euler に因んで **Euler 関数**と呼ばれている. この定義から, $\varphi(n)$ は集合 $\{0, 1, 2, \ldots, n-1\}$ (あるいは 0 の代わりに n を入れて $\{1, 2, \ldots, n\}$ を考えてもよい) に属する整数のうちで n と互いに素であるものの個数である.

命題 3.6. R を有限な可換環 (有限個の元を持つ可換環) とする. $|R^*| = k$ とすると, 全ての可逆元 $a \in R^*$ に対して $a^k = 1$ である.

証明. $a \in R^*$ とする. 写像 $f : R^* \to R^*$ を $f(x) = ax$ $(x \in R^*)$ で定める.[*11] $x, x' \in R^*$, $f(x) = f(x')$ とすると, $ax = ax'$ であるが, この両辺に逆元 a^{-1} を左から掛けて積の結合則を使えば

$$x = 1 \times x = (a^{-1}a)x = a^{-1}(ax) = a^{-1}(ax') = (a^{-1}a)x' = 1 \times x' = x'$$

が得られる. よって, f は単射である. ここで, R は有限集合だから, その部分集合である R^* も当然有限集合である. ゆえに, 第 2 巻『写像』命題 3.18 から f は全単射である. したがって,

$$\prod_{x \in R^*} x = \prod_{x \in R^*} f(x)$$

である. (左辺は全ての可逆元 $x \in R^*$ に渡る積であるが, 右辺の積はその項の順番を f に従って並べ替えただけのものである.) ここで, 右辺の積は

$$\prod_{x \in R^*} f(x) = \prod_{x \in R^*} (ax) = a^k \prod_{x \in R^*} x$$

である. ここで a^k が出てくるのは, x が R^* 全体で一巡させながら ax の積を取って行けば a が全部で $|R^*| = k$ 個現れるからである. よって, $\prod_{x \in R^*} x = a^k \prod_{x \in R^*} x$ であるが, この両辺に $\prod_{x \in R^*} x$ (これも一つの可逆元である) の逆元を掛ければ $a^k = 1$ が得られる. □

[*11] $a \in R^*$ なので, どの $x \in R^*$ についても $ax \in R^*$ である. だから, f は確かに R^* への写像である.

この命題 3.6 を剰余環 $\mathbb{Z}/n\mathbb{Z}$ に適用すれば, 次の定理が得られる.

Euler の定理

定理 3.7. $n \geq 2$ を自然数, a を整数とする. $\gcd(a,n) = 1$ ならば, n を法として $a^{\varphi(n)} \equiv 1$ である. つまり, $a^{\phi(n)} - 1$ は n の倍数である. ここで, φ は Euler 関数である.

証明. $\gcd(a,n) = 1$ と仮定する. 定理 3.4 から, 剰余類 $\pi(a) = a + n\mathbb{Z}$ は剰余環 $\mathbb{Z}/n\mathbb{Z}$ の可逆元である. すなわち, $\pi(a) \in (\mathbb{Z}/n\mathbb{Z})^*$ である. Euler 関数 φ の定義から $|(\mathbb{Z}/n\mathbb{Z})^*| = \varphi(n)$ なので, 命題 3.6 から $\pi(a)^{\varphi(n)} = \pi(1)$ である. これを整理すれば $\pi(a^{\varphi(n)}) = \pi(1)$, つまり $a^{\varphi(n)} \equiv 1$ が得られる. □

系 3.8 (Fermat の小定理)**.** p を素数, a を p の倍数ではない整数とするとき, p を法として $a^{p-1} \equiv 1$ である.

証明. 定理 3.7 を $n = p$ の場合に適用すればよい. p は素数なので, $a \notin p\mathbb{Z}$ は $\gcd(a,p) = 1$ と同じであること, そして $\varphi(p) = p - 1$ であることに注意すればよい. □

♦ **例 3.9**　$n = 15$ の場合を考える. $\mathbb{Z}/15\mathbb{Z}$ は 15 個の剰余類 $\pi(0), \pi(1), \ldots, \pi(14)$ から成る有限可換環である. 0 から 14 までの整数のうちで $n = 15$ と互いに素であるものは全部で $1, 2, 4, 7, 8, 11, 13, 14$ の 8 個あるので,

$$(\mathbb{Z}/15\mathbb{Z})^* = \{\pi(1), \pi(2), \pi(4), \pi(7), \pi(8), \pi(11), \pi(13), \pi(14)\}$$

であり, $\varphi(15) = |(\mathbb{Z}/15\mathbb{Z})^*| = 8$ である. 例えば,

$$\begin{aligned}
&\pi(4)^1 = \pi(4), \quad \pi(4)^2 = \pi(16) = \pi(1), \quad \pi(4)^8 = (\pi(3)^2)^4 = \pi(1), \\
&\pi(7)^1 = \pi(7), \quad \pi(7)^2 = \pi(49) = \pi(4), \quad \pi(7)^4 = (\pi(7)^2)^2 = \pi(16) = \pi(1), \\
&\pi(7)^8 = (\pi(7)^4)^2 = \pi(1)
\end{aligned}$$

などのようにして, 全ての $x \in (\mathbb{Z}/15\mathbb{Z})^*$ に対して $x^{\varphi(15)} = x^8 = \pi(1)$ であることが確かめられる. □

3.4 RSA 暗号

定理 3.7 は初等整数論における基本的な定理の一つであるが, 実はこれが公開鍵暗号方式の一つである RSA 暗号方式 (の最もプレーンな形のもの) の基本原理になっている. それについて簡単に触れておこう.

ここでは, もっぱら秘匿通信方式, すなわち秘密のメッセージをその中身を第三者に知られることなく相手に送り届けることを目的とした通信方式のことを「暗号方式」と呼ぶ.[*12] 暗号化される前の秘密メッセージを**平文**と言い, それに暗号化処理を施して作られるメッセージを**暗号文**と呼ぶ.

RSA 暗号方式では, 次の情報を使用する.

- 相異なる大きな素数 p, q およびそれらの積 $n = pq$.
- $\varphi(n)$ を法として $ed \equiv 1$ を満たす整数 e と d. ここで, φ は Euler 関数を表している.

[*12] 現代では, 秘匿通信の他にも電子署名や秘密計算, 秘密分散なども広く「暗号方式」と呼ばれていて, '暗号' が指す範囲は秘匿通信よりもだいぶ広い.

$n = pq$ は剰余環 $\mathbb{Z}/n\mathbb{Z}$ を指定する自然数である. RSA 暗号方式では, 全ての計算処理は剰余環 $\mathbb{Z}/n\mathbb{Z}$ 上で行われるが, 平文空間と暗号文空間は剰余環 $\mathbb{Z}/n\mathbb{Z}$ 全体ではなくて, その単数群 $(\mathbb{Z}/n\mathbb{Z})^*$ である. これは

$$(\mathbb{Z}/n\mathbb{Z})^* = \{\pi(a) \mid 0 \leq a < n,\ \gcd(a, n) = 1\}$$

という集合であり, 形式的には剰余類 $\pi(a) = a + n\mathbb{Z}$ らの集合であるが, 剰余類の集合というのがわかりにくければ, これを整数の集合

$$(\mathbb{Z}/n\mathbb{Z})^* = \{a \mid 0 \leq a < n,\ \gcd(a, n) = 1\}$$

だと考えても実質的には特に問題ない. (a は剰余類 $\pi(a) = a + n\mathbb{Z}$ を表す代表元だと思えばよい.) つまり, RSA 暗号方式では, 平文も暗号文も共に 0 から $n-1$ までの整数 (のうちで n と互いに素なもの) で表される. もちろん, 現実世界では平文は単なる数値ではなくて具体的な文字列 (メッセージ) であるが, それらが何らかの規則で整数としてコード化されていると仮定するわけである. ただし, 平文を整数としてコード化する操作は暗号化ではない. 同様に, 暗号文も整数であるが, それを具体的なメッセージに復元する操作は復号ではない. あくまで, 整数そのものを平文あるいは暗号文と見なして考える.

さて, 平文 $m \in (\mathbb{Z}/n\mathbb{Z})^*$ を暗号化するときには, 単にそれを e 乗する. つまり, 暗号化関数は

$$E : (\mathbb{Z}/n\mathbb{Z})^* \to (\mathbb{Z}/n\mathbb{Z})^*, \quad m \mapsto m^e$$

である. すると, 暗号文 $c \in (\mathbb{Z}/n\mathbb{Z})^*$ を復号する操作は e 乗根を求める操作に当たるはずだが, 一般に実数に対する e 乗根計算とは違って, $\mathbb{Z}/n\mathbb{Z}$ という '離散的' な空間における e 乗根の計算は簡単ではない. 実は, これから説明する通り, 復号関数, つまり e 乗根を求める関数は

$$D : (\mathbb{Z}/n\mathbb{Z})^* \to (\mathbb{Z}/n\mathbb{Z})^*, \quad c \mapsto c^d$$

で与えられる. すなわち, d 乗することが e 乗根を求める計算と同じことになる. これにはもちろん, e と d の選ばれ方にその秘密がある.

命題 3.10. E と D は互いに他方を逆関数とする全単射である.

証明. $D \circ E$ が恒等写像であることを示す. 任意の暗号文 $m \in (\mathbb{Z}/n\mathbb{Z})^*$ を取り, 暗号文を $c = E(m) = m^e$ とおく. これを復号すると $D(c) = m$ となることを示せばよい. D の定義から, $D(c) = c^d$ である. ここで, e と d は $\varphi(n)$ を法として $ed \equiv 1$ となるように選ばれているので, ある整数 k を用いて $ed - 1 = k\varphi(n)$, すなわち $ed = 1 + k\varphi(n)$ と書ける. (この k の値自身は大して重要ではなく, ed がこの形で書けるということが大切である.) すると, 指数法則を用いて

$$D(c) = c^d = (m^e)^d = m^{ed} = m^{1+k\varphi(n)} = m(m^{\varphi(n)})^k$$

と整理できる. ここで, $m \in (\mathbb{Z}/n\mathbb{Z})^*$ なので, 定理 3.7 から $(\mathbb{Z}/n\mathbb{Z})^*$ において $m^{\varphi(n)} = 1$ (単位元) が成り立つ. よって, $(m^{\varphi(n)})^k = 1^k = 1$ であり, したがって $D(c) = m$ が得られる. したがって, $D \circ E$ は恒等写像である. 同様の計算で, $E \circ D$ が恒等写像であることも言える. □

この命題で示された通り, 合成関数 $D \circ E$ は $(\mathbb{Z}/n\mathbb{Z})^*$ 上の恒等写像だから, 任意の平文 $m \in (\mathbb{Z}/n\mathbb{Z})^*$ を暗号化して暗号文 $c = E(m) = m^e$ を作り, それを復号関数で変換すれば $D(c) = D(E(m)) = m$ となって元の平文 m が正しく復号される. これが RSA 暗号方式の背後にある整数論的な仕掛けである.

暗号学的な事情あれこれ　以上は数学的観点のみからの話であるが, 実際に RSA 暗号方式が暗号方式として機能するためには, 他にいくつかの要件を考慮しておく必要がある.

まず, $n = pq$ はかなり大きな数である必要がある. と言うのも, n が小さいと平文空間および暗号文空間 $(\mathbb{Z}/n\mathbb{Z})^*$ が小さくなってしまう. 例えば, $n = 15$ ($p = 3$, $q = 5$) 程度だと平文および暗号文の種類は全部で $\varphi(15) = 8$ 通りしかない. ということは, 暗号文を見て元の平文が何かを全くデタラメに推測しても $1/8$ の確率で当たってしまうことになる. これでは, 暗号方式として安全だとはとても言えない. n が大きくなければ困る理由は他にもあるが, それはこれから徐々に説明していこう.

上記の説明から分かる通り, e は暗号化処理に用いられる**暗号化鍵**であり, d は復号処理に用いられる**復号鍵**である. (このように, 暗号化鍵と復号鍵が別々になっている暗号方式は**公開鍵暗号方式**と呼ばれている.) RSA 暗号方式では, 剰余環 $\mathbb{Z}/n\mathbb{Z}$ を指定する n および暗号化鍵 e は一般公開される. つまり, 暗号方式を攻撃しようとする攻撃者も含めて, 誰でも n と e を知ることができるというのが前提であり, したがって暗号化処理は誰でも実行できることが建前である.

一方で, d は復号のために使う鍵なので, これは明らかに正規の受信者のみの秘密にしておく必要がある. ところが, 実は $\varphi(n)$ の値が攻撃者にバレてしまうと, 次のようにして秘密復号鍵 d として働く情報が攻撃者に筒抜けになってしまう. まず, e と d は $\varphi(n)$ を法として $ed \equiv 1$ という関係にあったことを思い出そう. この関係から, 特に e と $\varphi(n)$ は互いに素である, つまり $\gcd(e, \varphi(n)) = 1$ であることが分かる. すると, 定理 3.3 から,

$$ex + \varphi(n)y = 1$$

を満たす整数 x, y が存在する. e は公開情報であり, $\varphi(n)$ も攻撃者の手に渡っているから, この方程式を立てること自体は攻撃者にも可能である. そして, これに整数解 (x, y) が '存在する' というだけであればいいのだが, 実はこの方程式を解いて実際に整数解 (x, y) を求めるための効率的なアルゴリズム (Euclid の**拡張互除法**) がある. それを用いれば, 攻撃者は整数解 (x, y) を得ることができる. ここで, $ex - 1 = \varphi(n)y$ なので, $\varphi(n)$ を法として $ex \equiv 1$ である. よって, x が復号鍵として機能してしまう.

こうして, $\varphi(n)$ の値が攻撃者にばれると攻撃者に秘密復号鍵 d を入手されてしまう. だから, $n = pq$ は公開するものの, $\varphi(n)$ の値は秘密にしておかなければいけない. さて, $n = pq$ であり, p と q は素数なので,

$$\varphi(n) = n - n/p - n/q + 1 = n - q - p - 1 = pq - q - p - 1 = (p-1)(q-1) \tag{7}$$

である. $\varphi(n)$ は 0 から $n-1$ までの整数で p とも q とも互いに素な整数の個数であるが, この範囲の中に p の倍数は $n/p = q$ 個, q の倍数は $n/q = p$ 個ある. よって, それら $p + q$ 個を排除しておき, $n - p - q$ が p とも q とも互いに素な整数の個数である…と言いたくなるが, これでは 0 を p の倍数かつ q の倍数として 2 回排除してしまっている. だから, それに 1 を加えて $\varphi(n) = n - p - q + 1$ とするのが正解である. それはともかく, 式 (7) によれば, n の素因数 p, q が攻撃者にバレると $\varphi(n)$ の値も簡単に攻撃者にバレてしまうことが分かる. だから, n は公開するが, その素因数 p, q は秘密にしておく必要がある. すなわち, n **をそう簡単に素因数分解されては困る**わけである. これが n が大きくなければいけないもう一つの理由であり,「RSA 暗号方式は大きな数の素因数分解が (計算量的な事情で) 難しいことに基づいている」と言われることの背景である.

計算機は大きな数どうしを掛け合わせることはもちろん得意だが, 意外なことにその逆操作, すなわち因数分解は計算機を用いても (現在のところは) 難しい. 例えば,

$$25195908475657893494027183240048398571429282126204032027777137836043662020707595556264018525880784406918290641249515082189298559149176184502808489120072$$

8449926873928072877767359714183472702618963750149718246911650776133798590957
0009733045974880842840179742910064245869181719511874612151517265463228221686
9987549182422433637259085141865462043576798423387184774447920739934236584823
8242811981638150106748104516603773060562016196762561338441436038339044149526
3443219011465754445417842402092461651572335077870774981712577246796292638635
6373289912154831438167899885040445364023527381951378636564391212010397122822
120720357

は 2 つの異なる素数の積であるが,[*13] これを素因数分解することは現在最速の計算機と現在のところ知られている最も性能のいいアルゴリズムを使っても簡単ではない. この辺りの事情は, 従来の計算機とは異なる仕組みを用いた量子計算機が実用化されるとガラっと変わってくるので, そうすると「$n = pq$ の素因数分解は難しい」という前提が崩れてしまう.

ところで, n の素因数 p, q がバレると $\varphi(n)$ の値も自動的にバレるが, n を素因数分解することなく $\varphi(n)$ の値を求める '抜け道' はないのだろうか? 実は, その心配はいらない. n から $\varphi(n)$ の値を求める手法があれば, それを使えば素因数 p, q を求めることができるからである. (ということは, n の素因数分解がバレない限り, n から $\varphi(n)$ がバレることはない.) $n = pq$ であり, 一方で $\varphi(n) = (p-1)(q-1) = n-(p+q)+1$, すなわち $p + q = n - \varphi(n) + 1$ なので,「解と係数の関係式」によれば, p と q は 2 次方程式

$$x^2 - (n - \varphi(n) + 1)x + n = 0$$

の解である. n は公開情報であり, そこから $\varphi(n)$ の値を求めることができれば, この 2 次方程式を立てることはできる. そして, もちろんそれを解くことも (解の公式を使えば) できる. こうして, n から $\varphi(n)$ を求めることができれば, 素因数 p と q が分かってしまう.

最後に, 暗号学における現代的な安全性基準から見ると, ここで説明したようなプレーンな形の RSA 暗号方式は十分に安全とは言えないので, 実際には乱数などを用いて安全性を高めるための改良が施された RSA 暗号方式が利用されていることを補足しておこう.

[*13] これは RSA-2048 Factoring Challenge の懸賞問題である. 10 進数で 617 桁, 2 進数表示で 2048 桁という莫大な数である.

付録 A　演習問題解答例

ここに示されているのはあくまで解答の一例であり, これだけが唯一絶対の正しい解答というわけではない. 参考程度の略解という位置付けである.

演習 1.1.　$(a,d) \in (R_3 \circ R_2 \circ) \circ R_1$ とすると, ある $b \in B$ が存在して, $(a,b) \in R_1$ かつ $(b,d) \in R_3 \circ R_2$ である. $(b,d) \in R_3 \circ R_2$ なので, ある $c \in C$ が存在して, $(b,c) \in R_2$ かつ $(c,d) \in R_3$ である. $(a,b) \in R_1$ と $(b,c) \in R_2$ から $(a,c) \in R_2 \circ R_1$ であり, これと $(c,d) \in R_3$ から $(a,d) \in R_3 \circ (R_2 \circ R_1)$ が従う. よって, $(R_3 \circ R_2) \circ R_1 \subseteq R_3 \circ (R_2 \circ R_1)$ である.

逆向きの包含を示そう. $(a,d) \in R_3 \circ (R_2 \circ R_1)$ とすると, ある $c \in C$ が存在して, $(a,c) \in R_1 \circ R_2$ かつ $(c,d) \in R_3$ である. $(a,c) \in R_1 \circ R_2$ なので, ある $b \in B$ が存在して, $(a,b) \in R_1$ かつ $(b,c) \in R_2$ である. $(b,c) \in R_2$ と $(c,d) \in R_3$ から $(b,d) \in R_3 \circ R_2$ であり, これと $(a,b) \in R_1$ から $(a,d) \in (R_3 \circ R_2) \circ R_1$ である. ゆえに, $(R_3 \circ R_2) \circ R_1 \supseteq R_3 \circ (R_2 \circ R_1)$ でもある. □

演習 1.2.　$(z,x) \in (R_2 \circ R_1)^{-1}$ とすると, $(x,z) \in R_2 \circ R_1$ だから, ある $y \in Y$ が存在して $(x,y) \in R_1$ かつ $(y,z) \in R_2$ となる. それぞれ $(z,y) \in R_2^{-1}$, $(y,x) \in R_1^{-1}$ なので, $(z,x) \in R_1^{-1} \circ R_2^{-1}$ が成り立つ. よって, $(R_2 \circ R_1)^{-1} \subseteq R_1^{-1} \circ R_2^{-1}$ である.

逆向きの包含を示す. $(z,x) \in R_1^{-1} \circ R_2^{-1}$ とすると, ある $y \in Y$ について $(z,y) \in R_2^{-1}$ かつ $(y,x) \in R_1^{-1}$ なので, $(x,y) \in R_1$ かつ $(y,z) \in R_2$, したがって $(x,z) \in R_2 \circ R_1$, つまり $(z,x) \in (R_2 \circ R_1)^{-1}$ である. よって, $(R_2 \circ R_1)^{-1} \supseteq R_1^{-1} \circ R_2^{-1}$ でもある. □

演習 1.3.　$X = Y = \mathbb{R}$, $R = \{(x,y) \mid x \leq y\}$ と定める. 任意の $(x,y) \in \mathbb{R}^2$ に対して,

$$\begin{aligned}(x,y) \in R \circ R^{-1} &\iff \text{ある } z \in \mathbb{R} \text{ について } (x,z) \in R^{-1} \text{ かつ } (z,y) \in R \\ &\iff \text{ある } z \in \mathbb{R} \text{ について } (z,x) \in R \text{ かつ } (z,y) \in R \\ &\iff \text{ある } z \in \mathbb{R} \text{ について } z \leq x \text{ かつ } z \leq y\end{aligned}$$

であるが, この最後の条件は $z = \min\{x,y\}$ に対して必ず成立する. よって, $R \circ R^{-1} = \mathbb{R}^2$ である. 同様に,

$$\begin{aligned}(x,y) \in R^{-1} \circ R &\iff \text{ある } z \in \mathbb{R} \text{ について } (x,z) \in R \text{ かつ } (z,y) \in R^{-1} \\ &\iff \text{ある } z \in \mathbb{R} \text{ について } (x,z) \in R \text{ かつ } (y,z) \in R \\ &\iff \text{ある } z \in \mathbb{R} \text{ について } z \leq x \text{ かつ } y \leq z \\ &\iff y \leq x \\ &\iff (y,x) \in R \\ &\iff (x,y) \in R^{-1}\end{aligned}$$

だから $R^{-1} \circ R = R^{-1} \neq \mathbb{R}^2 = R \circ R^{-1}$ である. □

演習 1.4.　(1) $R \subseteq R'$ であるとする. $(x,y) \in R^{-1}$ とすると, $(y,x) \in R$ であるが, 仮定から $R \subseteq R'$ だから $(y,x) \in R'$ でもあり, したがって $(x,y) \in R'^{-1}$ である. よって, $R^{-1} \subseteq R'^{-1}$ である.

(2) (1) から, $(R \cap R')^{-1} \subseteq R^{-1} \cap R'^{-1}$ である. この逆向きの包含を示す. $(x,y) \in R^{-1} \cap R'^{-1}$ とする. $(x,y) \in R^{-1}$ だから, $(y,x) \in R$ である. 同じく, $(x,y) \in R'^{-1}$ だから, $(y,x) \in R'$ である. よって, $(y,x) \in R \cap R'$ であり, すなわち $(x,y) \in (R \cap R')^{-1}$ である. ゆえに, $(R \cap R')^{-1} \supseteq R^{-1} \cap R'^{-1}$ でもある.

(3) (1) から, $(R\cup R')^{-1}\supseteq R^{-1}\cup R'^{-1}$ である. この逆向きの包含を示す. $(x,y)\in(R\cup R')^{-1}$ とすると, $(y,x)\in R\cup R'$ であるが, $(y,x)\in R$ または $(y,x)\in R'$ であることに応じてそれぞれ $(x,y)\in R^{-1}$ または $(x,y)\in R'^{-1}$ が成り立つので, $(x,y)\in R^{-1}\cup R'^{-1}$ である. よって, $(R\cup R')^{-1}\subseteq R^{-1}\cup R'^{-1}$ でもある. □

演習 1.5.　(1) $A\cap A=A\neq\emptyset$ なので, $A\sim A$ である. ゆえに, $\sim$ は反射的である.

$A\sim B\iff A\cap B\neq\emptyset\iff B\cap A\neq\emptyset\iff B\sim A$ なので, $\sim$ は対称的である.

$A=\{1,2\}$, $B=\{2,3\}$ に対して $A\sim B$ かつ $B\sim A$ であるが, $A\neq B$ である. よって, $\sim$ は反対称的ではない.

$A=\{1,2\}$, $B=\{2,3\}$, $C=\{3,4\}$ に対して $A\sim B$ かつ $B\sim C$ であるが, $A\cap C=\emptyset$ なので $A\sim C$ ではない. よって, $\sim$ は推移的ではない.

(2) $x/x=1$ なので, $x\sim x$ である. よって, $\sim$ は反射的である.

$x/y\in\mathbb{Q}$ であれば, $y/x=(x/y)^{-1}\in\mathbb{Q}$ でもあるので, $x\sim y\Rightarrow y\sim x$ である. よって, $\sim$ は対称的である.

$3/2, 2/3\in\mathbb{Q}$ だから, $2\sim 3$ かつ $3\sim 2$ であるが, $2\neq 3$ である. よって, $\sim$ は反対称的ではない.

$x\sim y$, $y\sim z$ とすると, $x/y, y/z\in\mathbb{Q}$ なので, $x/z=(x/y)(y/z)\in\mathbb{Q}$, よって $x\sim z$ である. ゆえに, $\sim$ は推移的である. □

演習 1.6.　(1) $X=\{1,2,3\}$ とおくと, $R=\{(1,1),(1,2),(2,1),(2,2)\}$ は対称的かつ推移的ではあるが, $(3,3)\notin R$ だから反射的ではない.

(2) $X=\{1,2,3\}$ とおくと, $R=\{(1,1),(1,2),(2,1),(2,2),(2,3),(3,2),(3,3)\}$ は反射的かつ対称的であるが, $(1,2),(2,3)\in R$ かつ $(1,3)\notin R$ だから推移的ではない.

(3) $\mathbb{Z}$ 上の通常の大小関係 $x\leq y$ は反射的かつ推移的であるが, $3\leq 5$ なのに $5\leq 3$ ではないので対称的ではない. □

演習 1.7.　(1) $X=\{1,2,3\}$ とおく. $R=\{(1,1),(2,2)\}$ は対称的かつ反対称的であるが, $(3,3)\notin R$ だから反射的ではない.

(2) 最初に $x\sim y$ となる y を選ぶところに問題がある. そのような y が存在する保証は一般にはない. 実際, (1) の例では $x=3$ に対して y が取れない. □

演習 1.8.　$(x,y)\in R_{\mathrm{trans}}$ とすると, X の有限個の点から成る列 $x=x_0,x_1,\ldots,x_n=y$ が存在して, 全ての $1\leq k\leq n$ に対して $(x_{k-1},x_k)\in R$ が成り立つ. R は対称的だから, 各々の k について $(x_k,x_{k-1})\in R$ である. したがって, 列 $x=x_0,x_1,\ldots,x_n=y$ を右から左に読めば $(y,x)\in R_{\mathrm{trans}}$ であることがわかる. よって, R_{trans} は対称的である. □

演習 1.9.　(1) $x=\{1,2\}$, $y=\{2,3\}$, $z=\{3,4\}$ とおくと, $x\sim y$ かつ $y\sim z$ であるが, $x\sim z$ ではない. よって, $\sim$ は推移的ではない.

(2) $x,y\in X$ とする. x, y は空集合ではないので, それぞれ自然数 $a\in x$, $b\in y$ を選ぶことができる. $w=\{a,b\}$ とおく. $a\in x\cap w$ だから, $x\sim w$ である. 一方, $b\in w\cap y$ だから, $w\sim y$ でもある. よって, $x\approx y$ である. □

演習 2.1.　まず $\equiv$ が同値関係であることを確かめる.

- 反射性: $A \in \mathrm{GL}_n(\mathbb{R})$ に対して, $S = I$ (単位行列) を取れば $A = AS$, $S \in \mathrm{SL}_n(\mathbb{R})$ である.
- 対称性: $A = BS$, $S \in \mathrm{SL}_n(\mathbb{R})$ とすると, $B = AS^{-1}$, $S^{-1} \in \mathrm{SL}_n(\mathbb{R})$ である.
- 推移性: $A = BS$, $B = CT$, $S, T \in \mathrm{SL}_n(\mathbb{R})$ とすると, $A = BS = (CT)S = C(TS)$, $TS \in \mathrm{SL}_n(\mathbb{R})$ である.

□

演習 2.2.　反射性: $m = n = 1$ に対して $f^m(x) = f^n(x)$ だから $x \equiv x$ である.

対称性: $x \equiv y$ とすると, ある $m, n \in \mathbb{N}$ について $f^m(x) = f^n(y)$ なので, $f^n(y) = f^m(x)$ でもあり, $y \equiv x$ である.

推移性: $x \equiv y$, $y \equiv z$ とすると, ある $m, n, k, l \in \mathbb{N}$ について $f^m(x) = f^n(y)$, $f^k(y) = f^l(z)$ である. すると, $f^{mk}(x) = f^{nk}(y) = f^{nl}(z)$ となるので $x \equiv z$ である. □

演習 2.3.　(1) 反射閉包と対称閉包の定義から,

$$\begin{aligned}
(R_{\mathrm{ref}})_{\mathrm{sym}} &= R_{\mathrm{ref}} \cup (R_{\mathrm{ref}})^{-1} \\
&= (R \cup \Delta_X) \cup (R \cup \Delta_X)^{-1} \\
&= (R \cup \Delta_X) \cup (R^{-1} \cup \Delta_X^{-1}) && \text{(演習 1.4(3))} \\
&= (R \cup R^{-1}) \cup (\Delta_X \cup \Delta_X^{-1}) \\
&= R_{\mathrm{sym}} \cup \Delta_X && (\Delta_X^{-1} = \Delta_X) \\
&= (R_{\mathrm{sym}})_{\mathrm{ref}}
\end{aligned}$$

である.

(2) R の反射対称閉包を S とし, その推移閉包を $\bar{R} = S_{\mathrm{trans}}$ とおく. $\bar{R}$ は S の推移閉包なので推移的である. S は対称的だから, 演習 1.8 からその推移閉包たる $\bar{R}$ も対称的である. S は反射的なので, $\Delta_X \subseteq S \subseteq \bar{R}$ であり, $\bar{R}$ も反射的である. さらに, $R \subseteq S \subseteq \bar{R}$ でもある. よって, $\bar{R}$ は R を含む同値関係である. T が R を含む同値関係ならば, T は R を含みかつ反射的かつ対称的な関係であるが, S はそのような最小の関係だから $S \subseteq T$ である. そして, T は推移的なので, $\bar{R} = S_{\mathrm{trans}} \subseteq T_{\mathrm{trans}} = T$ である. ゆえに, $\bar{R}$ は R を含む最小の同値関係である. □

演習 2.4.　(1) $A \equiv B$ と仮定して, $A = BS$ ($S \in \mathrm{SL}_n(\mathbb{R})$) と書くと, $\det A = \det(BS) = \det B \cdot \det S = \det B$ である. 逆に, $\det A = \det B$ とすると, $S = B^{-1}A$ に対して $\det S = (\det B)^{-1}(\det A) = 1$ だから, $S \in \mathrm{SL}_n(\mathbb{R})$ であり, $A = BS$ だから, $A \equiv B$ である.

(2) 0 でない任意の実数 r について, n 次単位行列の $(1,1)$-成分のみを r に置き換えて得られる行列を P_r とする. P_r の行列式はその全ての対角成分の積なので r である. $\mathcal{P} = \{P_r \mid r \neq 0\}$ は完全代表系であることを示す. $A \in \mathrm{GL}_n(\mathbb{R})$ として, その行列式を r とすると, (1) から $A \equiv P_r$ である. 次に, r, r' を 0 でない実数, $P_r \equiv P_{r'}$ とすると, (1) から両辺の行列式を見れば $r = r'$ であることがわかる. よって, $\mathcal{P}$ は完全代表系である. □

演習 2.5.　任意の $A, B \in \mathcal{P}$ について,

$$\begin{aligned} A \equiv B &\iff |A \vartriangle B| \text{ が偶数} \\ &\iff |A \cup B| - |A \cap B| \text{ が偶数} \\ &\iff |A \cup B| + |A \cap B| \text{ が偶数} \\ &\iff |A| + |B| \text{ が偶数} \\ &\iff |A| \text{ と } |B| \text{ の偶奇が同じ} \end{aligned}$$

である. このことから, $\equiv$ が同値関係であることはすぐにわかる. さらに, $\mathcal{P} = \{\emptyset, \{1\}\}$ は完全代表系である. ($\emptyset$ が偶数個の元から成る部分集合らの代表であり, $\{1\}$ が奇数個の元から成る部分集合の代表である.) □

演習 2.6.　(1) 格子点の全体を $L = \{a + bi \mid a, b \in \mathbb{Z}\}$ で表す. 任意の $u, v \in L$ について, $u + v, -v \in L$ であることに注意しておく.

- 任意の $z \in \mathbb{C}$ について, $z - z = 0 \in L$ なので, $z \equiv z$ である. よって, $\equiv$ は反射的である.
- $w, z \in \mathbb{C}$, $w \equiv z$ とすると, $w - z \in L$ なので, $z - w = -(w - z) \in L$, したがって $z \equiv w$ でもある. よって, $\equiv$ は対称的である.
- $w, y, z \in \mathbb{C}$, $w \equiv y$ かつ $y \equiv z$ とすると, $w - y \in L$, $y - z \in L$ なので, $w - z = (w - y) + (y - z) \in L$ であり, したがって $w \equiv z$ である. よって, $\equiv$ は推移的である.

以上から, $\equiv$ は同値関係である.

(2) 任意の $z = x + iy \in \mathbb{C}$ ($z = \mathfrak{R}z$, $y = \mathfrak{I}z$) について, $a = \lfloor x \rfloor$, $b = \lfloor y \rfloor$, $w = (x - a) + (y - b)i$ とおく. (実数 r に対して, $\lfloor r \rfloor$ は r 以下で最大の整数を表す.) すると, $x - a, y - b \in [0, 1)$ だから $w \in I$ であり, なおかつ $z - w = a + ib \in L$ なので $z \equiv w$ である. 次に, $w, z \in I$, $w \equiv z$ とすると, $w - z$ は格子点であるが, $w, z \in I$ だから, $w - z$ の実部と虚部は共に区間 $(-1, 1)$ に属する整数, すなわち 0 であるしかなく, $w - z = 0$, つまり $w = z$ である. よって, I は完全代表系である. □

演習 2.7.　$\pi : X \to \bar{X}$ は類別写像を表すものとする.

(1) $\bar{f}$ が単射であると仮定する. $x \equiv x'$ ならば $f(x) = f(x')$ であることは f が $\equiv$ を保つことから従う. 逆に, $f(x) = f(x')$ であるとすると, 商写像 $\bar{f}$ の定義から $\bar{f}(\pi(x)) = f(x) = f(x') = \bar{f}(\pi(x'))$ となるが, $\bar{f}$ は単射なので $\pi(x) = \pi(x')$, すなわち $x \equiv x'$ である.

逆に, $x \equiv x' \iff f(x) = f(x')$ であると仮定する. $\bar{f}(\pi(x)) = \bar{f}(\pi(x'))$ とすると, $f(x) = \bar{f}(\pi(x)) = \bar{f}(\pi(x')) = f(x')$ なので, 仮定から $x \equiv x'$, つまり $\pi(x) = \pi(x')$ である. ゆえに, $\bar{f}$ は単射である.

(2) $\bar{f}$ が全射ならば, 任意の $y \in Y$ に応じて $\bar{f}(C) = y$ を満たす $C \in \bar{X}$ が存在する. C が点 $x \in X$ の同値類だとすると, $C = \pi(x)$ だから, $y = \bar{f}(C) = \bar{f}(\pi(x)) = f(x)$ である. よって, f は全射である. 逆に f が全射ならば, 任意の $y \in Y$ に応じて, $f(x) = y$ となる $x \in X$ を取れば $y = f(x) = \bar{f}(\pi(x))$ となるから $\bar{f}$ も全射である. □

演習 2.8.　X 上に同値関係 $x \equiv x' \iff f(x) = f(x')$ を設定して, それによる商集合を Z, 類別写像を $u : X \to Z$ で定める. u は全射である. $\equiv$ の定義から f は $\equiv$ を保つので, f の商写像 $v : Z \to Y$ が定まる. 演習 2.7(1) から v は単射である. そして, 任意の $x \in X$ について $f(x) = v(u(x))$ だから, $f = v \circ u$ である. □