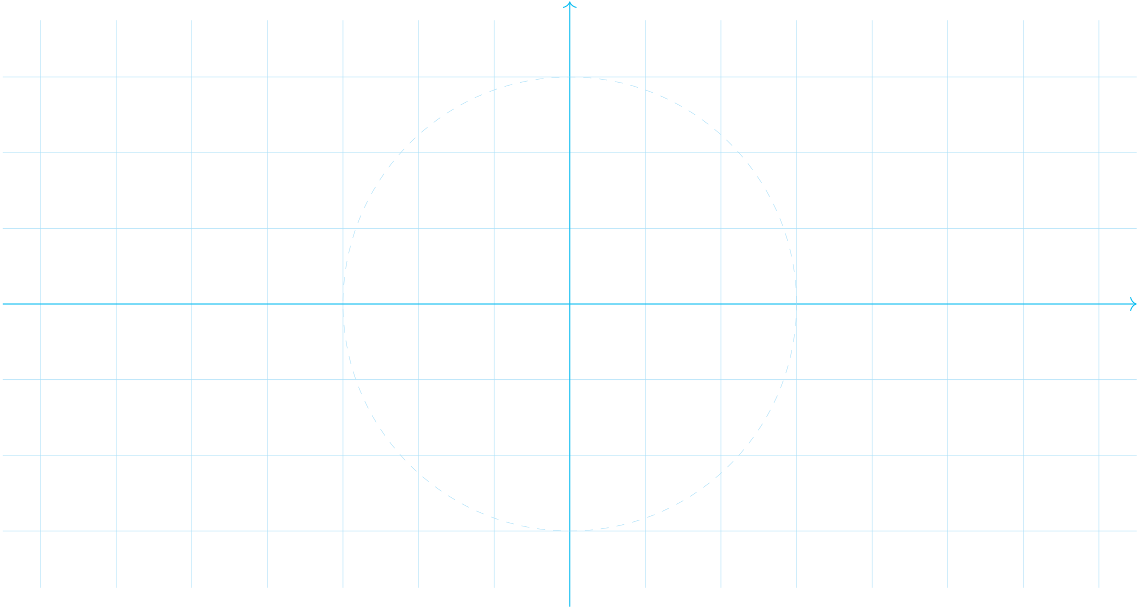
memo



離散数学

授業開始までしばらくお待ちください。

2024

離散数学

Discrete Mathematics

『写像』

bit.ly/d-math

小林裕之

大阪工業大学 RD 学部システムデザイン工学科

OSAKA INSTITUTE OF TECHNOLOGY

8 of 14

a LaTeX + Beamer slideshow

授業の受講に関して

- 講義資料（スライド等）は **Google Drive** (`https://bit.ly/d-math`) に置く (紙の配布資料は行わない)。授業前には虫喰い状態のスライドのみを提供するが、授業後に `uncovered`フォルダに穴埋め版を置くので復習に活用されたい。
- ミニレポートは**Google Forms** (`https://forms.gle/hCyJBbFBMW9AisAt7`) に提出。
- 授業の録画はできるだけスライドと同じフォルダ内のフォルダに置くように努力する（が、必ず置きますとお約束はしません)。
- 授業中に計算間違い等を指摘してくれたらその都度 1 点。(内容に依るけど。)

成績評価について

- 出席そのものは評価せず。極論するとテストのみ出席で他は全欠席でも A 評価はあり得る。
- 基本的には**中間演習**と**期末試験**で評価。
- 毎回ミニレポートを課す。出す者は提出期間を厳守すること。
- 試験の不合格者は**毎回のミニレポート**と**出席**で少し救済する。
  (**しっかりした内容の**ミニレポートを概ね 9 割以上提出し、かつ大学の出欠管理システムで 8 割以上遅刻せず出席していた場合最大 10 点程度の救済。提出数や出席数が少ない場合は救済幅が縮小する。いずれかが 7 割を下回ったら一切救済しない。締め切り後の提出は認めない。)
- **授業中に**スライドの誤りを見つけて指摘してくれた者には、誤り一箇所につき先着一名様限り 100 点満点 1 点相当の加点を行う。(ただしごく軽微なものなど、内容によっては加点しない場合もあり。)

写像

写像

A から B への**関係**の特殊ケース

写像 (mapping; “関数”, “変換” とも。)

集合 A から集合 B への**関係**のうち、**任意の A の要素**に対して、B の要素が **ただ一つ**対応しているものを写像という。

- A:
- B:
- 書き方: ,

写像

A から B への関係の特殊ケース

写像 (mapping; “関数”, “変換” とも。)

集合 A から集合 B への**関係**のうち、**任意の A の要素**に対して、B の要素が **ただ一つ**対応しているものを写像という。

- A: 定義域
- B:
- 書き方: ,

写像

A から B への**関係**の特殊ケース

写像 (mapping; “関数”, “変換” とも。)

集合 A から集合 B への**関係**のうち、**任意の A の要素**に対して、B の要素が **ただ一つ**対応しているものを写像という。

- A: 定義域
- B: 値域 (像)
- 書き方: ,

写像 (mapping; “関数”, “変換” とも。)

集合 A から集合 B への**関係**のうち、**任意の A の要素**に対して、B の要素が **ただ一つ**対応しているものを写像という。

- A: 定義域
- B: 値域 (像)
- 書き方: $f : A \to B$,

写像

A から B への**関係**の特殊ケース

写像 (mapping; “関数”, “変換” とも。)

集合 A から集合 B への**関係**のうち、**任意の A の要素**に対して、B の要素が **ただ一つ**対応しているものを写像という。

- A: 定義域
- B: 値域 (像)
- 書き方: $f : A \to B, \quad b = f(a) \ \ (a \in A, b \in B)$

ワークシート: 「写像」関係を描いてみよう。

単射, 全射, 全単射

単射

全射

全単射

単射, 全射, 全単射

単射

$$(\forall a_1, a_2 \in A) f(a_1) = f(a_2) \to a_1 = a_2$$

全射

全単射

単射, 全射, 全単射

単射

$$(\forall a_1, a_2 \in A)\, f(a_1) = f(a_2) \to a_1 = a_2$$

全射

$$(\forall b \in B,\ \exists a \in A)\, b = f(a)$$

全単射

単射, 全射, 全単射

単射

$$(\forall a_1, a_2 \in A)\, f(a_1) = f(a_2) \to a_1 = a_2$$

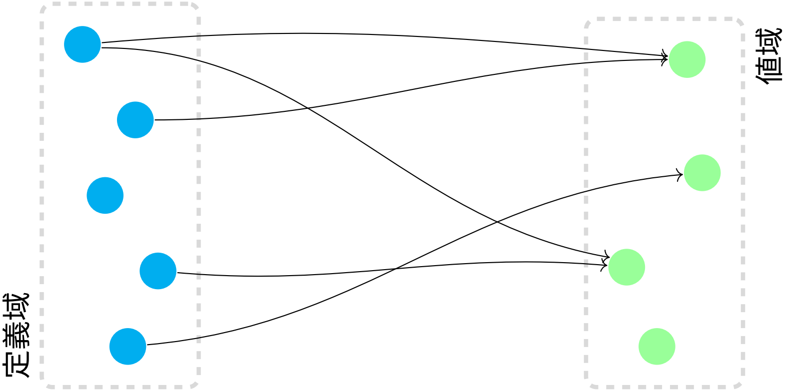
全射

$$(\forall b \in B,\ \exists a \in A)\, b = f(a)$$

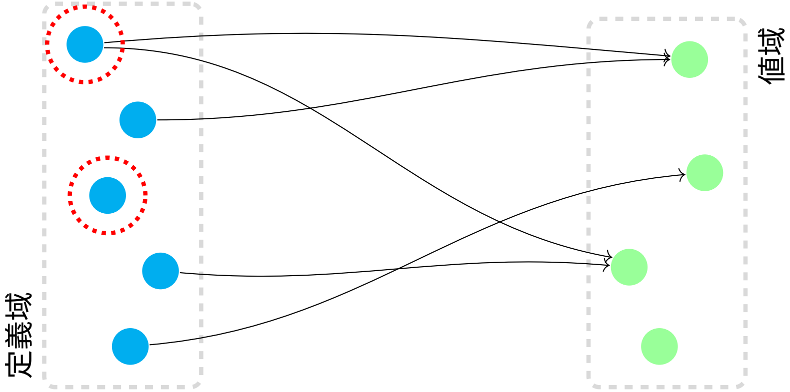
全単射

全射かつ単射

《図解》全射, 単射, 全単射 (1 of 4) ～写像でない～

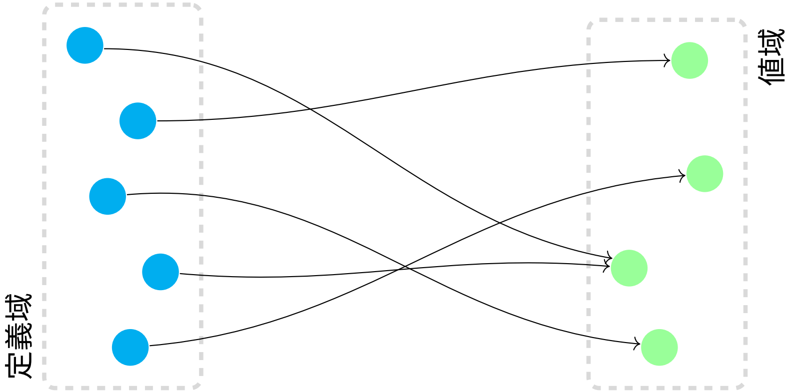


《図解》全射, 単射, 全単射 (1 of 4) 〜写像でない〜



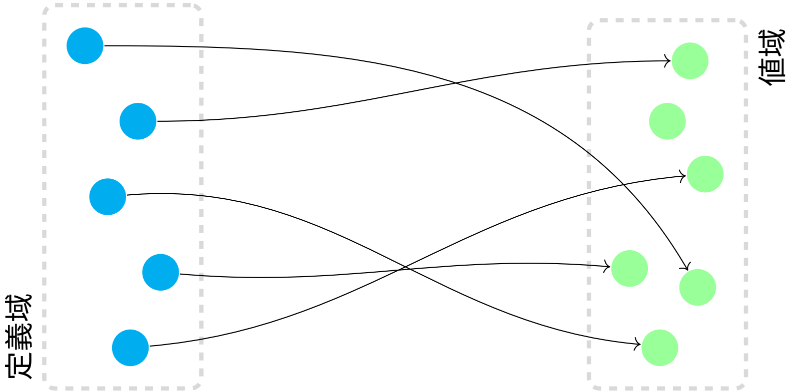
定義域の要素からは**必ず、もれなく、きっちり１本**矢印が伸びる。
したがって、上図はそもそも**写像でない**。

《図解》全射, 単射, 全単射 (2 of 4) 〜全射〜



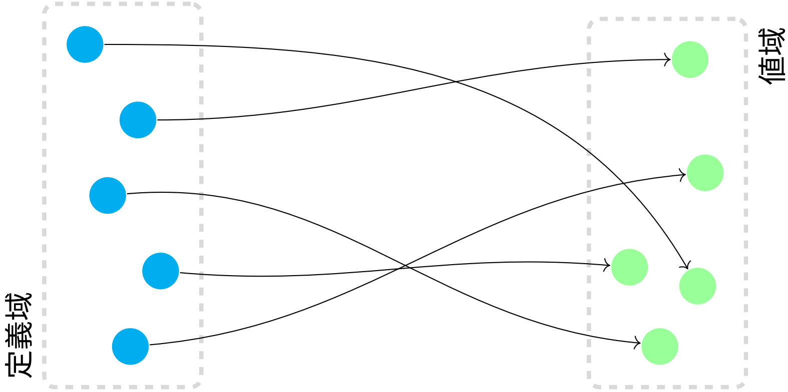
写像かつ、値域の**全**ての要素に 1 本以上矢印が入っていれば**全射**。

《図解》全射, 単射, 全単射 (3 of 4) 〜単射〜



写像かつ、値域の全ての要素に入ってくる矢印が**1本以下**(単)であれば**単射**。(つまり、(値域には) 余り者がいてもいい。)

《図解》全射, 単射, 全単射 (4 of 4) ～全単射～



定義域と値域の全ての要素が**もれなく 1 対 1 対応**していれば
全単射。

逆写像 (AKA 逆関数, 逆変換)

$f : A \to B$ の逆関係 $f^{-1} : B \to A$ が写像になっているとき、f^{-1} は f の**逆写像**という。

写像・逆写像クイズ

$\mathbb{R} \to \mathbb{R}$ の写像 $f(x) = x^2$ は全射あるいは単射か? また、逆関係 f^{-1} は写像か?

写像 f の逆関係 f^{-1} が写像であるための必要十分条件は f が　　　　であることである。

逆写像 (AKA 逆関数, 逆変換)

$f: A \to B$ の逆関係 $f^{-1}: B \to A$ が写像になっているとき、f^{-1} は f の**逆写像**という。

写像・逆写像クイズ

$\mathbb{R} \to \mathbb{R}$ の写像 $f(x) = x^2$ は全射あるいは単射か? また、逆関係 f^{-1} は写像か?

単射でも全射でもない。逆関係は写像でない。

写像 f の逆関係 f^{-1} が写像であるための必要十分条件は f が　　　　であることである。

逆写像 (AKA 逆関数, 逆変換)

$f : A \to B$ の逆関係 $f^{-1} : B \to A$ が写像になっているとき、f^{-1} は f の**逆写像**という。

写像・逆写像クイズ

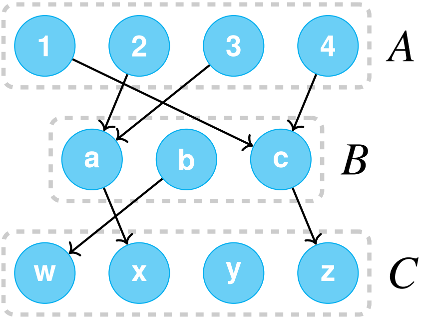
$\mathbb{R} \to \mathbb{R}$ の写像 $f(x) = x^2$ は全射あるいは単射か? また、逆関係 f^{-1} は写像か?

単射でも全射でもない。逆関係は写像でない。

写像 f の逆関係 f^{-1} が写像であるための必要十分条件は f が**全単射**であることである。

合成写像

合成関係とおなじ



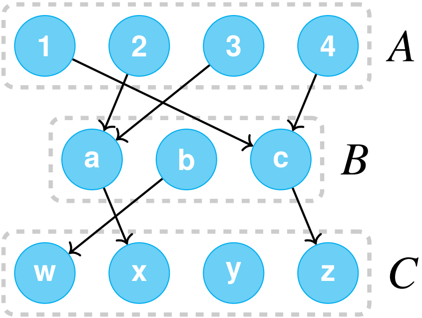
- 「A から B への写像 f」と「B から C への写像 g」を合成した、「　から　への写像」を　　といい、　　と表す[a]。
- 左図の場合、

$$g \circ f = \{ \qquad \}$$

[a]順番に注意。

合成写像

合成関係とおなじ

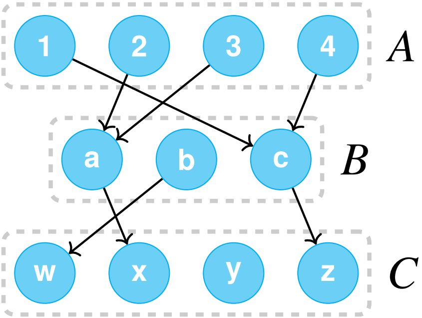


- 「A から B への写像 f」と「B から C への写像 g」を合成した、「Aから Cへの写像」を　　　　といい、　　　　と表す[a]。
- 左図の場合、

$$g \circ f = \{ \qquad\qquad\qquad\qquad \}$$

[a]順番に注意。

合成写像
合成関係とおなじ



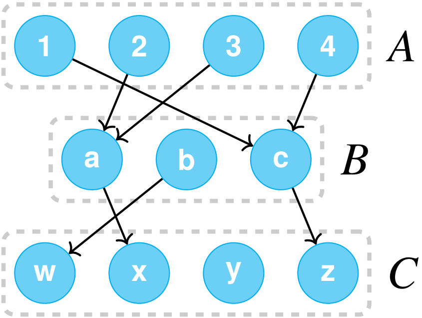
- 「A から B への写像 f」と「B から C への写像 g」を合成した、「Aから Cへの写像」を**合成写像**といい、　　と表す[a]。
- 左図の場合、

$$g \circ f = \{ \qquad\qquad\qquad\qquad \}$$

[a]順番に注意。

合成写像

合成関係とおなじ



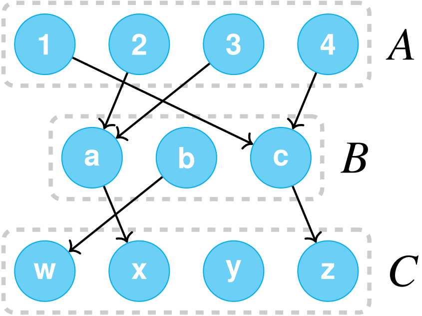
- 「A から B への写像 f」と「B から C への写像 g」を合成した、「Aから Cへの写像」を**合成写像**といい、$g \circ f$と表す[a]。
- 左図の場合、

$$g \circ f = \{ \qquad \qquad \qquad \qquad \qquad \qquad \}$$

[a]順番に注意。

合成写像

合成関係とおなじ



- 「A から B への写像 f」と「B から C への写像 g」を合成した、「Aから Cへの写像」を**合成写像**といい、$g \circ f$と表す[a]。
- 左図の場合、

  $g \circ f = \{\langle 1, z\rangle, \langle 2, x\rangle, \langle 3, x\rangle, \langle 4, z\rangle\}$

[a]順番に注意。

写像の性質

全射・単射は引き継がれるのか？

クイズ

- f, g が全単射なら $g \circ f$ も全単射と言えるか?
- f, g が単射なら $g \circ f$ も単射と言えるか?
- f, g が全射なら $g \circ f$ も全射と言えるか?

クイズ

- f, g が全単射なら $g \circ f$ も全単射と言えるか?

  yes

- f, g が単射なら $g \circ f$ も単射と言えるか?

- f, g が全射なら $g \circ f$ も全射と言えるか?

クイズ

- f, g が全単射なら $g \circ f$ も全単射と言えるか?

  yes
- f, g が単射なら $g \circ f$ も単射と言えるか?

  yes
- f, g が全射なら $g \circ f$ も全射と言えるか?

クイズ

- f, g が全単射なら $g \circ f$ も全単射と言えるか?

  yes
- f, g が単射なら $g \circ f$ も単射と言えるか?

  yes
- f, g が全射なら $g \circ f$ も全射と言えるか?

  yes

コラム: プログラミング言語における “関数”

C 言語の関数は関数ではない?

関数(つまり写像) は、「定義域のある要素」から「**ただ一つの**(値域の) 要素」が決まる関係であった。つまり $f(a)$ と書いたら、値は一意に決まる必要がある。(当たり前と思う?)

一方プログラミング言語 (例えば C 言語) の “関数” は、**引数が一定でも戻り値が一定とは限らない**。例えばこんなの:

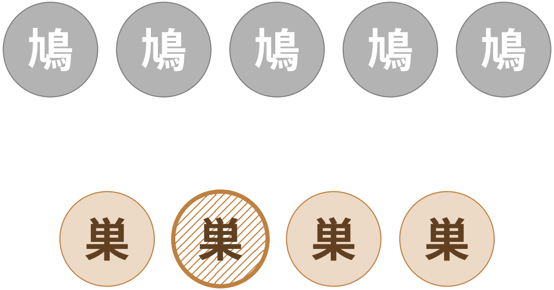
```c
int f(int x) {
  static int a = 0;
  a++;
  return x + a;
}
```

こういうのは良くない、という考えのもと、原則として数学の関数のような関数しか許さない**純粋関数型言語**という種類のプログラミング言語もある (例: Haskell)。

鳩の巣原理

当たり前のことだけど、応用はいろいろ。

A から B の写像が、『全射ならば $|A| \quad |B|$』『**単射ならば** $|A| \quad |B|$』『全単射ならば $|A| \quad |B|$』。この 2 つめの**対偶**が**鳩の巣原理** (pigeonhole principle)

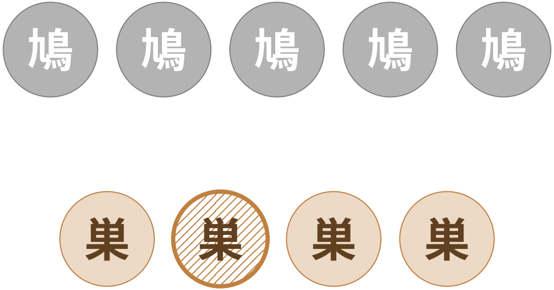


← 鳩が多ければ必ず 2 羽以上の巣が発生する。

鳩の巣原理

当たり前のことだけど、応用はいろいろ。

A から B の写像が、『全射ならば $|A| \geq |B|$』『**単射ならば** $|A| \quad |B|$』『全単射ならば $|A| \quad |B|$』。この 2 つめの**対偶**が**鳩の巣原理** (pigeonhole principle)

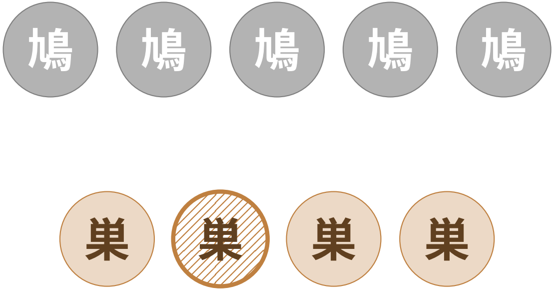


← 鳩が多ければ必ず 2 羽以上の巣が発生する。

鳩の巣原理

当たり前のことだけど、応用はいろいろ。

A から B の写像が、『全射ならば $|A| \geq |B|$』『**単射ならば $|A| \leq |B|$**』『全単射ならば $|A| \quad |B|$』。この 2 つめの**対偶**が**鳩の巣原理** (pigeonhole principle)

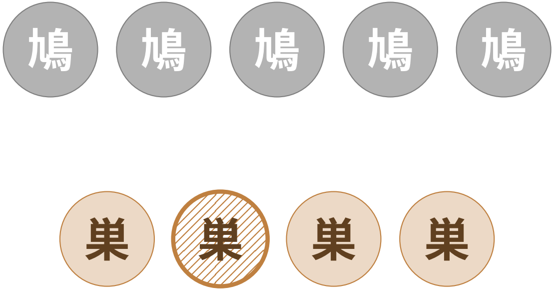


← 鳩が多ければ必ず 2 羽以上の巣が発生する。

鳩の巣原理

当たり前のことだけど、応用はいろいろ。

A から B の写像が、『全射ならば $|A| \geq |B|$』『**単射ならば $|A| \leq |B|$**』『全単射ならば $|A| = |B|$』。この 2 つめの**対偶**が**鳩の巣原理** (pigeonhole principle)

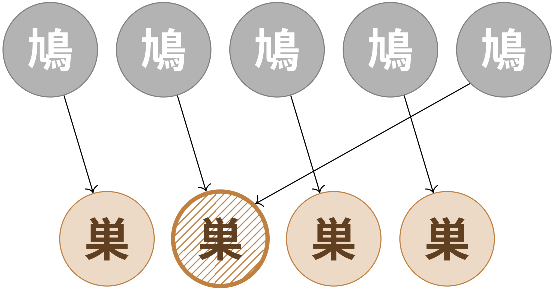


← 鳩が多ければ必ず 2 羽以上の巣が発生する。

鳩の巣原理

当たり前のことだけど、応用はいろいろ。

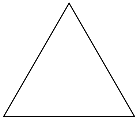
A から B の写像が、『全射ならば $|A| \geq |B|$』『**単射ならば $|A| \leq |B|$**』『全単射ならば $|A| = |B|$』。この 2 つめの**対偶**が**鳩の巣原理** (pigeonhole principle)



← 鳩が多ければ必ず 2 羽以上の巣が発生する。

クイズ

1. 人には平均 10 万本もの髪の毛がある。大阪市内に髪の毛の本数がぴったり等しい二人が存在する確率はどの程度か。
2. 1 辺が 1 m の正三角形の中に互いに 50 cm 離して 5 つの点は打てないことを示せ。



3. zip, rar, 7z などなど、世の中には数多くの可逆圧縮アルゴリズムが存在するが、どのアルゴリズムにも必ずそれぞれ圧縮不可能な (オリジナルより小さくできない) データというものが存在することを示せ。

一方向ハッシュ関数
セキュリティ技術の要

- 有限長の任意のデータ (ビット列) の集合から、一定のビット列 (例えば 128 ビット) のデータへの写像。
- 定義域を**メッセージ**、値域を**ハッシュ値**という。
- メッセージの正真性の検査に使う。(例: 電子署名)
- パスワードの保存にも使う。
- 逆関係が推定しにくく、**衝突**しにくいほど良い。
- MD5, SHA-1, SHA-2 が有名。(MD5, SHA-1 は脆弱性があるため現在では非推奨。)

(全ページで出てきた) 『衝突』とは

- 異なるメッセージが同一の　　　　　を生成することを『衝突』(collision) という。
- ハッシュ関数で衝突は**必ず発生する**。(なぜならば　　　　　　があるので。)
- 使用状況に応じて衝突の発生確率を減らすことが重要。
- ビ　　　　　ンの　　　　　　　ではSHA-2で衝突を起こすデータを探すのに近いこと[a]をしている。

[a] 完全な「衝突」ではなく、狭い範囲に入るいわば「ニアミス」。(本当に故意に衝突させられたらそれはSHA-2の脆弱性になり世界中がひっくり返っちゃいます…。)

(全ページで出てきた) 『衝突』とは

- 異なるメッセージが同一のハッシュ値を生成することを『衝突』という。 (collision)
- ハッシュ関数で衝突は**必ず発生する**。(なぜならば　があるので。)
- 使用状況に応じて衝突の発生確率を減らすことが重要。
- ビ　ンの　ではSHA-2で衝突を起こすデータを探すのに近いこと[a]をしている。

---

[a]完全な「衝突」ではなく、狭い範囲に入るいわば「ニアミス」。(本当に故意に衝突させられたらそれはSHA-2の脆弱性になり世界中がひっくり返っちゃいます…。)

(全ページで出てきた) 『衝突』とは

- 異なるメッセージが同一のハッシュ値を生成することを『衝突』(collision) という。
- ハッシュ関数で衝突は**必ず発生する**。(なぜならば**鳩の巣原理**があるので。)
- 使用状況に応じて衝突の発生確率を減らすことが重要。
- ビ　　　　ンの　　　　　　では SHA-2 で衝突を起こすデータを探すのに近いこと[a]をしている。

[a]完全な「衝突」ではなく、狭い範囲に入るいわば「ニアミス」。(本当に故意に衝突させられたらそれは SHA-2 の脆弱性になり世界中がひっくり返っちゃいます…。)

(全ページで出てきた)『衝突』とは

- 異なるメッセージが同一のハッシュ値を生成することを『衝突』(collision)という。
- ハッシュ関数で衝突は**必ず発生する**。(なぜならば**鳩の巣原理**があるので。)
- 使用状況に応じて衝突の発生確率を減らすことが重要。
- ビットコインの　　　　　　　　　　ではSHA-2で衝突を起こすデータを探すのに近いこと[a]をしている。

[a]完全な「衝突」ではなく、狭い範囲に入るいわば「ニアミス」。(本当に故意に衝突させられたらそれはSHA-2の脆弱性になり世界中がひっくり返っちゃいます…。)

(全ページで出てきた)『衝突』とは

- 異なるメッセージが同一のハッシュ値 を生成することを『衝突』(collision) という。
- ハッシュ関数で衝突は**必ず発生する**。(なぜならば**鳩の巣原理**があるので。)
- 使用状況に応じて衝突の発生確率を減らすことが重要。
- ビットコインのマイニング では SHA-2 で衝突を起こすデータを探すのに近いこと[a] をしている。

[a] 完全な「衝突」ではなく、狭い範囲に入るいわば「ニアミス」。(本当に故意に衝突させられたらそれは SHA-2 の脆弱性になり世界中がひっくり返っちゃいます…。)

置換

$\{1, 2, \ldots, n\}$ をn **次の置換**という。

置換の表し方:

$f = \{\langle 1, 3\rangle, \langle 2, 1\rangle, \langle 3, 4\rangle, \langle 4, 5\rangle, \langle 5, 2\rangle\}$ の例 ↓

置換

$\{1, 2, \ldots, n\}$上の　　　　　　　　　　をn **次の置換**という。

置換の表し方:

$f = \{\langle 1, 3\rangle, \langle 2, 1\rangle, \langle 3, 4\rangle, \langle 4, 5\rangle, \langle 5, 2\rangle\}$ の例 $\downarrow$

置換

$\{1, 2, \ldots, n\}$上の全単射写像をn **次の置換**という。

置換の表し方:

$f = \{\langle 1, 3\rangle, \langle 2, 1\rangle, \langle 3, 4\rangle, \langle 4, 5\rangle, \langle 5, 2\rangle\}$ の例 ↓

置換

$\{1, 2, \ldots, n\}$上の全単射写像をn **次の置換**という。

置換の表し方:

$f = \{\langle 1, 3\rangle, \langle 2, 1\rangle, \langle 3, 4\rangle, \langle 4, 5\rangle, \langle 5, 2\rangle\}$ の例 ↓

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 5 & 2 \end{pmatrix}$$

置換についていろいろ

簡単な話とどこかで聞いたような話ばかりなので軽く流しましょう。

- 同一元どうしが対応しているものを　　　　　という。
- n 次の置換全体を　と表す。
- $|S_n| =$
- S_n 上の置換 σ と φ を連続して適用する置換を『σ と φ の　』といい、　　　と表す。
- 置換 σ の逆写像を　　　　　といい、　　と表す。

- 同一元どうしが対応しているものを **恒等置換** という。
- n 次の置換全体を　と表す。
- $|S_n| =$
- S_n 上の置換 σ と φ を連続して適用する置換を『σ と φ の　』といい、　　　と表す。
- 置換 σ の逆写像を　　　　といい、　　と表す。

置換についていろいろ

簡単な話とどこかで聞いたような話ばかりなので軽く流しましょう。

- 同一元どうしが対応しているものを **恒等置換** という。
- n 次の置換全体を S_n と表す。
- $|S_n| =$
- S_n 上の置換 σ と φ を連続して適用する置換を『σ と φ の　』といい、　　　と表す。
- 置換 σ の逆写像を　　　　といい、　　と表す。

置換についていろいろ

簡単な話とどこかで聞いたような話ばかりなので軽く流しましょう。

- 同一元どうしが対応しているものを **恒等置換** という。
- n 次の置換全体をS_nと表す。
- $|S_n| = n!$
- S_n 上の置換 σ と φ を連続して適用する置換を『σ と φ の　』といい、　　　　と表す。
- 置換 σ の逆写像を　　　　　といい、　　　と表す。

置換についていろいろ

簡単な話とどこかで聞いたような話ばかりなので軽く流しましょう。

- 同一元どうしが対応しているものを **恒等置換**という。
- n 次の置換全体をS_nと表す。
- $|S_n| = n!$
- S_n 上の置換 σ と φ を連続して適用する置換を『σ と φ の**積**』といい、と表す。
- 置換 σ の逆写像をといい、と表す。

置換についていろいろ

簡単な話とどこかで聞いたような話ばかりなので軽く流しましょう。

- 同一元どうしが対応しているものを **恒等置換** という。
- n 次の置換全体をS_nと表す。
- $|S_n| = n!$
- S_n 上の置換 σ と φ を連続して適用する置換を『σ と φ の**積**』といい、$\varphi \circ \sigma$と表す。
- 置換 σ の逆写像を　　　　といい、　　と表す。

置換についていろいろ

簡単な話とどこかで聞いたような話ばかりなので軽く流しましょう。

- 同一元どうしが対応しているものを **恒等置換**という。
- n 次の置換全体をS_nと表す。
- $|S_n| = n!$
- S_n 上の置換 σ と φ を連続して適用する置換を『σ と φ の**積**』といい、$\varphi \circ \sigma$と表す。
- 置換 σ の逆写像を**逆置換**といい、　　と表す。

置換についていろいろ

簡単な話とどこかで聞いたような話ばかりなので軽く流しましょう。

- 同一元どうしが対応しているものを **恒等置換**という。
- n 次の置換全体をS_nと表す。
- $|S_n| = n!$
- S_n 上の置換 σ と φ を連続して適用する置換を『σ と φ の**積**』といい、$\varphi \circ \sigma$と表す。
- 置換 σ の逆写像を**逆置換**といい、σ^{-1}と表す。

互換

恒等置換の次に単純な置換?

- 2 要素を入れ替える置換を　　　という。
- 互換は入れ替える 2 要素だけを $(2\ 4)$ のように書くこともできる。

$$(2\ 4) = \begin{pmatrix} 1 & \mathbf{2} & 3 & \mathbf{4} & 5 \\ 1 & \mathbf{4} & 3 & \mathbf{2} & 5 \end{pmatrix}$$

- **任意の置換は互換の積で表せる。**(ただし一意ではない。)

互換

恒等置換の次に単純な置換?

- 2 要素を入れ替える置換を**互換**という。
- 互換は入れ替える 2 要素だけを (2 4) のように書くこともできる。

$$(2\ 4) = \begin{pmatrix} 1 & \mathbf{2} & 3 & \mathbf{4} & 5 \\ 1 & \mathbf{4} & 3 & \mathbf{2} & 5 \end{pmatrix}$$

- **任意の置換は互換の積で表せる。**(ただし一意ではない。)

練習問題 (5 分)

1. 置換の積を計算せよ。

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

2. $\{1, 2, 3, 4\}$ 上の互換の積を計算せよ。

$$(1\ 4)(1\ 3)(1\ 2) =$$

3. 置換を互換の積にせよ。(解は一意ではない。)

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

練習問題 (5 分)

1. 置換の積を計算せよ。

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

2. $\{1, 2, 3, 4\}$ 上の互換の積を計算せよ。

$$(1\ 4)(1\ 3)(1\ 2) =$$

3. 置換を互換の積にせよ。(解は一意ではない。)

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

練習問題 (5 分)

1. 置換の積を計算せよ。

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

2. $\{1, 2, 3, 4\}$ 上の互換の積を計算せよ。

$$(1\ 4)(1\ 3)(1\ 2) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

3. 置換を互換の積にせよ。(解は一意ではない。)

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

練習問題 (5 分)

1. 置換の積を計算せよ。

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

2. $\{1, 2, 3, 4\}$ 上の互換の積を計算せよ。

$$(1\ 4)(1\ 3)(1\ 2) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

3. 置換を互換の積にせよ。(解は一意ではない。)

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix} = (2\ 4)(1\ 4)$$

可算濃度

だいぶ前にやったことをあらためて。

2 つの集合の間に　　　　写像が存在するならば、その 2 つは同じ濃度である。

- ℕ と同じ濃度を持つ集合の濃度を　　　　(記号で　) という。
- 無限集合の濃度のうち最小のものが　　　　である。

可算濃度

だいぶ前にやったことをあらためて。

2 つの集合の間に全単射写像が存在するならば、その 2 つは同じ濃度である。

- $\mathbb{N}$ と同じ濃度を持つ集合の濃度を　　　　(記号で　)という。
- 無限集合の濃度のうち最小のものが　　　　である。

可算濃度

だいぶ前にやったことをあらためて。

> **2 つの集合の間に全単射写像が存在するならば、その 2 つは同じ濃度である。**

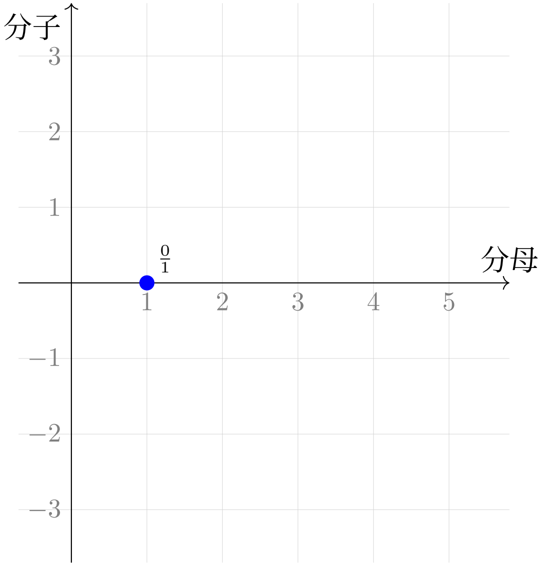
- $\mathbb{N}$ と同じ濃度を持つ集合の濃度を**可算濃度**(記号で) という。
- 無限集合の濃度のうち最小のものが**可算濃度**である。

可算濃度

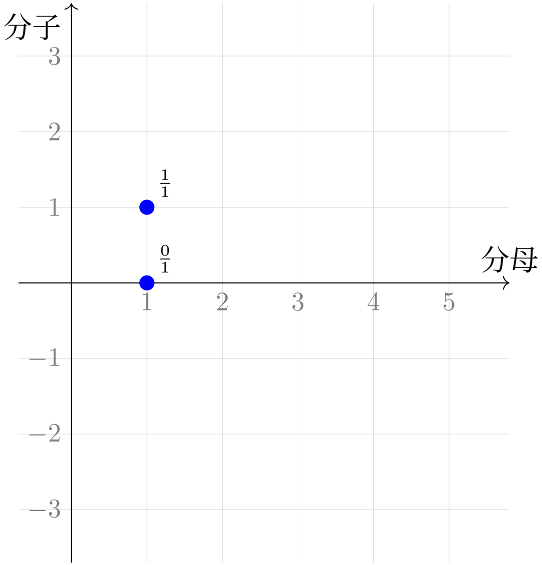
だいぶ前にやったことをあらためて。

2 つの集合の間に全単射写像が存在するならば、その 2 つは同じ濃度である。

- $\mathbb{N}$ と同じ濃度を持つ集合の濃度を**可算濃度**(記号で$\aleph_0$) という。
- 無限集合の濃度のうち最小のものが**可算濃度**である。

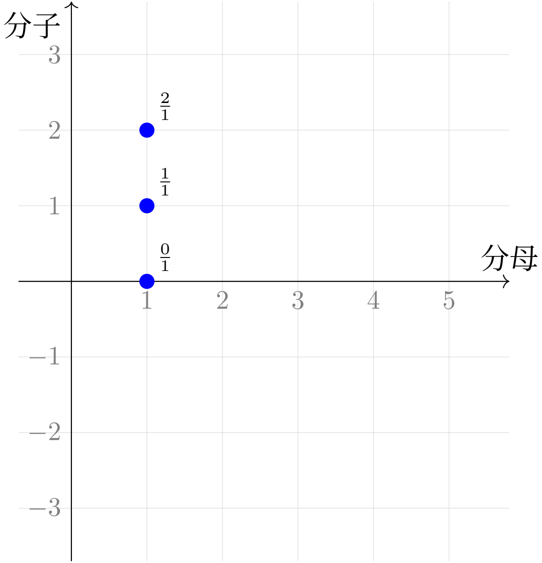


1. 分母 (> 0) と分子の座標系を書く。
2. $\forall q_i \in \mathbb{Q}$ は必ずどこかにある。
3. すべての q_i に 1 から順番に一意の番号を振ればそれが全単射。
   ($|\mathbb{Q}| =$)

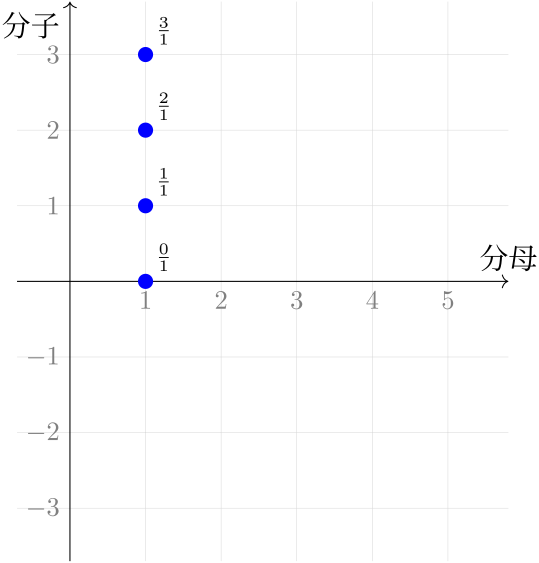


1. 分母 (> 0) と分子の座標系を書く。
2. $\forall q_i \in \mathbb{Q}$ は必ずどこかにある。
3. すべての q_i に 1 から順番に一意の番号を振ればそれが全単射。
   $(|\mathbb{Q}| = \qquad\qquad)$

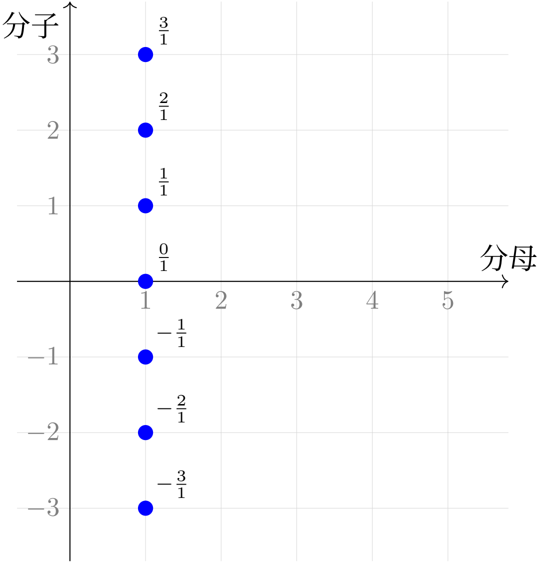
$\mathbb{Q}$ と $\mathbb{N}$



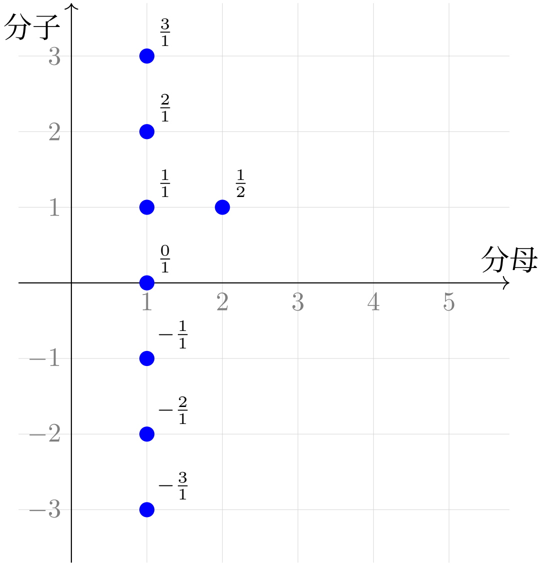
1. 分母 (> 0) と分子の座標系を書く。
2. $\forall q_i \in \mathbb{Q}$ は必ずどこかにある。
3. すべての q_i に 1 から順番に一意の番号を振ればそれが全単射。
   $(|\mathbb{Q}| = \qquad\qquad)$



1. 分母 (> 0) と分子の座標系を書く。
2. $\forall q_i \in \mathbb{Q}$ は必ずどこかにある。
3. すべての q_i に 1 から順番に一意の番号を振ればそれが全単射。 $(|\mathbb{Q}| = \qquad\qquad)$

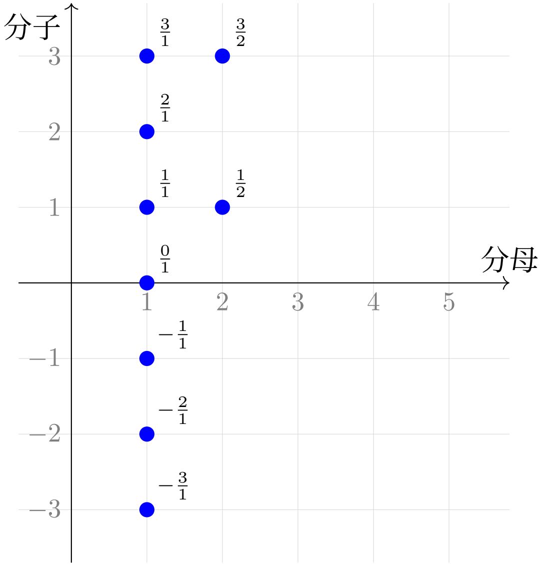


1. 分母 (> 0) と分子の座標系を書く。
2. $\forall q_i \in \mathbb{Q}$ は必ずどこかにある。
3. すべての q_i に 1 から順番に一意の番号を振ればそれが全単射。
   $(|\mathbb{Q}| =$ $)$



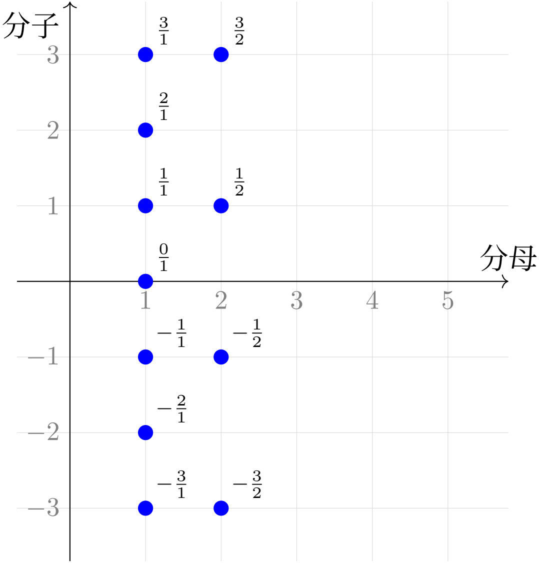
1. 分母 (> 0) と分子の座標系を書く。
2. $\forall q_i \in \mathbb{Q}$ は必ずどこかにある。
3. すべての q_i に 1 から順番に一意の番号を振ればそれが全単射。
   $(|\mathbb{Q}| = \qquad\qquad)$

$\mathbb{Q}$ と $\mathbb{N}$



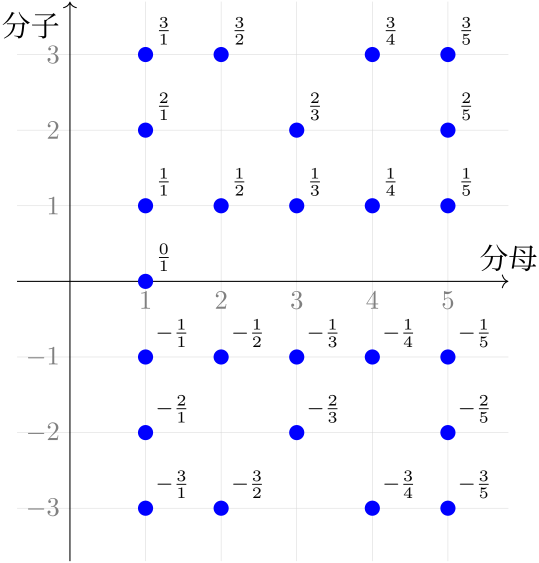
1. 分母 (>0) と分子の座標系を書く。
2. $\forall q_i \in \mathbb{Q}$ は必ずどこかにある。
3. すべての q_i に 1 から順番に一意の番号を振ればそれが全単射。

$(|\mathbb{Q}| = \qquad\qquad)$



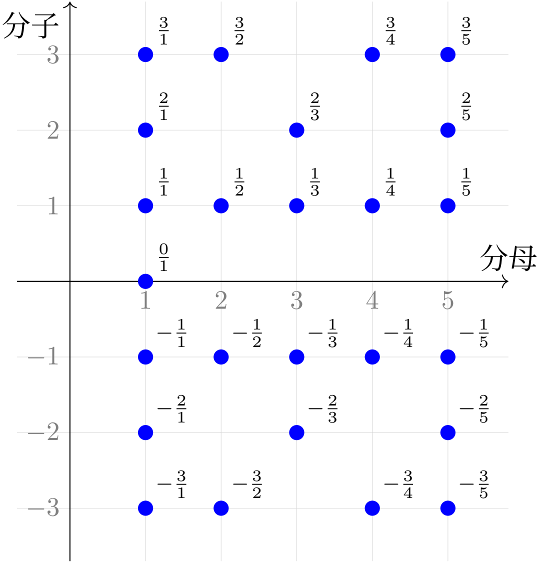
1. 分母 (> 0) と分子の座標系を書く。
2. $\forall q_i \in \mathbb{Q}$ は必ずどこかにある。
3. すべての q_i に 1 から順番に一意の番号を振ればそれが全単射。
($|\mathbb{Q}| =$)

$\mathbb{Q}$ と $\mathbb{N}$



1. 分母 (> 0) と分子の座標系を書く。
2. $\forall q_i \in \mathbb{Q}$ は必ずどこかにある。
3. すべての q_i に 1 から順番に一意の番号を振ればそれが全単射。
   $(|\mathbb{Q}| = \qquad\qquad)$

$\mathbb{Q}$ と $\mathbb{N}$



1. 分母 (> 0) と分子の座標系を書く。
2. $\forall q_i \in \mathbb{Q}$ は必ずどこかにある。
3. すべての q_i に 1 から順番に一意の番号を振ればそれが全単射。 $(|\mathbb{Q}| = |\mathbb{N}| = \aleph_0)$

突然ですがプログラミング演習 (なぜここで？)

問: アルファベット 4 文字の文字列を 4 個入力すると、それらの**どれとも異なる A, B の組み合わせ 4 文字**を 1 つ出力するプログラムを作れ。

実行例

```
$ python3 fourwords.py
MOON     # <- 入力 1
FIRE     # <- 入力 2
TREE     # <- 入力 3
AQUA     # <- 入力 4
AAAB     # <- 出力
```

そりゃまあ確かにどれとも違うけど…。

解答例 (Python(上) と Ruby(下))

突然ですがプログラミング演習 (なぜここで？)

問: アルファベット 4 文字の文字列を 4 個入力すると、それらの**どれとも異なる A, B の組み合わせ 4 文字**を 1 つ出力するプログラムを作れ。

実行例

```
$ python3 fourwords.py
MOON     # <- 入力 1
FIRE     # <- 入力 2
TREE     # <- 入力 3
AQUA     # <- 入力 4
AAAB     # <- 出力
```

そりゃまあ確かにどれとも違うけど…。

解答例 (Python(上) と Ruby(下))

```python
ans = ""
for i in range(4):
  ans += ("A" if input()[i] != "A"
           else "B")
print(ans)
```

```ruby
puts (0..3).inject('') {|s, i|
  s + (gets[i] != 'A' ? 'A' : 'B')
}
```

実数の無限桁表現の話 (またまたなぜここで？)

問: 正しい関係演算子を 1 つ選びなさい。

$$0.99\cdots \quad \begin{matrix} > \\ = \\ < \end{matrix} \quad 1$$

実数の無限桁表現の話 (またまたなぜここで？)

問: 正しい関係演算子を 1 つ選びなさい。

$$0.99\cdots \begin{matrix} > \\ = \\ < \end{matrix} 1$$

そして、Cantor（カントール）降臨。

練習

問に答えよ。

1. $\mathbb{N} \to \{0, 1\}$ の写像 $f(x) = x \bmod 2$ は全射・単射・全単射か。ただし mod 2 は 2 で割った余りとする。
2. $\mathbb{R} \to [-1, 1]$ の写像 $f(\theta) = \cos\theta$ は全射・単射・全単射か。
3. S_2 を具体的に示せ。
4. $\mathbb{Z}$ が可算濃度を持つことを示すために、なんでもいいので $\mathbb{Z} \to \mathbb{N}$ の全単射写像を考えよ。

練習

問に答えよ。

1. $\mathbb{N} \to \{0, 1\}$ の写像 $f(x) = x \bmod 2$ は全射・単射・全単射か。ただし mod 2 は 2 で割った余りとする。
2. $\mathbb{R} \to [-1, 1]$ の写像 $f(\theta) = \cos\theta$ は全射・単射・全単射か。
3. S_2 を具体的に示せ。
4. $\mathbb{Z}$ が可算濃度を持つことを示すために、なんでもいいので $\mathbb{Z} \to \mathbb{N}$ の全単射写像を考えよ。

略解: 1. 全射, 2. 全射, 3. $\left\{ \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\}$

ミニレポート課題 (提出期間: 本日〜次回の授業の前日)

前ページの問題を解け。

解答を PC 文書や手書きで作成し、PDF にして Google Forms (**https://forms.gle/hCyJBbFBMW9AisAt7**) から提出せよ (要組織アカウントによるログイン)。ただし写真等の画像ファイルの場合は、解像度や露出・照明状態などを十分考慮し、きちんと読解可能なクオリティのものとすること。スマートフォンの場合はスキャナアプリの類の利用を必須とする。