

情報数理 B

土谷 昭善 (akiyoshi@is.sci.toho-u.ac.jp)

目次

1	情報数理 A の復習 (集合と論理)	1
1.1	直積集合	1
1.2	論理	1
1.3	集合族	2
1.4	演習問題	2
2	情報数理 A の復習 (写像)	3
2.1	写像	3
2.2	全射と単射	3
2.3	演習問題	4
3	二項関係	5
3.1	二項関係	5
3.2	矢線図と有向グラフ	5
3.3	二項関係の演算	6
3.4	逆関係	6
3.5	合成関係	7
4	同値関係	9
4.1	反射的な関係	9
4.2	対称的な関係	9
4.3	推移的な関係	10
4.4	同値関係	11
4.5	合同式	12
5	同値類と商集合	13
5.1	集合の分割	13
5.2	同値類と商集合	13
5.3	同値関係と分割	15
5.4	一般角	15
5.5	小数部分	16
6	順序関係と順序集合	17
6.1	前順序	17
6.2	反対称的な関係	17
6.3	半順序	18
6.4	ハッセ図	19
7	最大・最小/極大・極小/上界・下界/上限・下限	21
7.1	極大・極小/最大・最小	21
7.2	上界・下界/上限・下限	22
8	束	25
8.1	束	25
8.2	結びと交わり	26
8.3	分配束とモジュー束	27

9	自然数	29
9.1	自然数の定義	29
9.2	自然数の加法	30
9.3	自然数の乗法	31
9.4	半群とモノイド	32
10	整数	33
10.1	整数の定義	33
10.2	整数の加法と乗法	33
10.3	整数の減法	35
10.4	群と環	36
11	有理数	37
11.1	有理数の定義	37
11.2	有理数の加法, 乗法	37
11.3	有理数の除法	38
11.4	体	39
11.5	有理数上の順序	39
11.6	実数と複素数	40

1 情報数理 A の復習 (集合と論理)

1.1 直積集合

数学の表現方法として直積集合という概念がある。その定義を復習する。要素の順序対 (ordered pair) (a, b) を考える。 a は第 1 成分と呼ばれ、 b は第 2 成分と呼ばれる。このとき $a = b$ でないならば、 $(a, b) \neq (b, a)$ である。さらに、 $(a, b) = (c, d)$ となるのは、 $a = c$ かつ $b = d$ のときで、かつこのときに限る。2 つの任意の集合 A と B を考える。すべての順序対 (a, b) ($a \in A, b \in B$) の集合は、 A と B の直積 (direct product) と呼ばれ、 $A \times B$ と表す。定義より、

$$A \times B = \{(a, b) : a \in A, b \in B\}$$

となる。また、しばしば $A \times A$ の代わりに、 A^2 と書く。順序対の概念を拡張すると、 n 個の順序付けられた成分の組 $(a_1, a_2, a_3, \dots, a_n)$ を要素として持つ直積集合が定義できる。

$$A_1 \times A_2 \times \dots \times A_n = \{(a_1, a_2, a_3, \dots, a_n) : a_1 \in A_1, a_2 \in A_2, \dots, a_n \in A_n\}$$

$$A^n = A \times A \times \dots \times A = \{(a_1, a_2, a_3, \dots, a_n) : a_1, a_2, \dots, a_n \in A\}$$

直積集合は例えば次のような例を表したいときに使う。

1. xy 平面の全ての点の集合は $\mathbb{R}$ を実数の集合として、 $\mathbb{R}^2 = \{(x, y) : x, y \in \mathbb{R}\}$ と表せる。また xyz 空間内の全ての点の集合は $\mathbb{R}^3 = \{(x, y, z) : x, y, z \in \mathbb{R}\}$ と表せる。これを拡張した n 個の実数の組の集まり $\mathbb{R}^n = \{(x_1, x_2, \dots, x_n) : x_1, x_2, \dots, x_n \in \mathbb{R}\}$ を n 次元実空間という。
2. コンピュータ上で一般的に用いられる色の集合は X を 0 以上 255 以下の自然数の集合とし、集合 R を赤の成分の大きさを表す集合、集合 G を緑の成分の大きさを表す集合、集合 B を青の成分の大きさを表す集合として、 $R \times G \times B = \{(r, g, b) : r, g, b \in X\}$ と表せる。

このように直積集合はいくつかのデータの組を扱うときに使う。一方で、一つの対象をいくつかの成分に分解するときに使うことも多い。例えば、複素数の全体の集合を $\mathbb{C}$ としたとき、複素数 $x \in \mathbb{C}$ は実数 $a, b \in \mathbb{R}$ を使って、 $x = a + b\sqrt{-1}$ と表すことができる。この $x \in \mathbb{C}$ と $(a, b) \in \mathbb{R}^2$ の対応により、 $\mathbb{C}$ は $\mathbb{R}^2$ と同一視できる。複素平面はこの対応を考えている。

1.2 論理

数学の証明の基本は、ある命題 P を仮定して、新しい命題 Q が成り立つこと、つまり推論

$$P \Rightarrow Q$$

を証明することである。よく使う性質として以下のものが挙げられる。

- $\neg P \wedge \neg Q \Leftrightarrow \neg(P \vee Q)$ (ド・モルガンの法則)
- $\neg P \vee \neg Q \Leftrightarrow \neg(P \wedge Q)$ (ド・モルガンの法則)
- $P \wedge Q \Rightarrow P$
- $P \Rightarrow P \vee Q$
- $(P \rightarrow Q) \Leftrightarrow \neg P \vee Q$
- $(P \rightarrow Q) \wedge P \Leftrightarrow P \wedge Q$
- $(P \rightarrow Q) \wedge (Q \rightarrow R) \Rightarrow (P \rightarrow R)$ (三段論法)
- $(P \rightarrow Q) \Leftrightarrow (\neg Q \rightarrow \neg P)$ (対偶)

変数 (variable) x を含む命題 $P(x)$ を述語という。述語は変数 x に具体的な値を代入することによって命題となる。変数を増やして $P(x_1, x_2, \dots, x_n)$ という命題も考えられる。述語 $P(x)$ に対して、「すべての x について $P(x)$ である」という命題を全称命題といい、 $\forall x(P(x))$ と書く。 $\forall$ は全称記号と呼ばれる (for all を表す)。また、述語 $P(x)$ に対して、「ある x について $P(x)$ である」という命題を存在命題といい、 $\exists x(P(x))$ と書く。 $\exists$ は存在記号と呼ばれる (exist を表す)。複数の変数に対して $\forall$ または $\exists$ が連続で出てくる場合、例えば、 $\forall x(\exists y(P(x, y)))$ の場合は $\forall x \exists y(P(x, y))$ のように記号の前のカッコを省略する。 $\forall$ と $\exists$ の両方が連続で出てくる場合、その順番で意味が変わることに注意する。

1.3 集合族

集合を要素として持つ集合を**集合族** (family of sets) と呼ぶ. 添字集合を Λ とする集合族 $\{A_\lambda\}_{\lambda \in \Lambda}$ の共通部分 $\bigcap_{\lambda \in \Lambda} A_\lambda$ と合併 $\bigcup_{\lambda \in \Lambda} A_\lambda$ を

$$x \in \bigcap_{\lambda \in \Lambda} A_\lambda \stackrel{\text{def}}{\Leftrightarrow} \forall \lambda \in \Lambda (x \in A_\lambda), \quad x \in \bigcup_{\lambda \in \Lambda} A_\lambda \stackrel{\text{def}}{\Leftrightarrow} \exists \lambda \in \Lambda (x \in A_\lambda)$$

で定義する. 添字集合が自然数全体の集合 $\mathbb{N}$ のときは, $\bigcap_{k=1}^{\infty} A_k$ や $\bigcup_{k=1}^{\infty} A_k$ とも書く. また添字集合を定めずに集合族 $\mathcal{A}$ の共通部分と合併を考えるときは $\bigcap_{X \in \mathcal{A}} X$ や $\bigcup_{X \in \mathcal{A}} X$ とも書く.

1.4 演習問題

1. $A = \{1, 2, 3\}$ と $B = \{a, b\}$ が与えられているとき, 以下をそれぞれ求めよ.

- (a) $A \times B$
- (b) $B \times A$
- (c) $B \times B$

2. 複素数の集合 $\mathbb{C}$ は $\mathbb{R}^2$ と同一視できると説明したが, 実際は $\mathbb{R}^2$ を複素数と思うために $\mathbb{R}^2$ の演算を考える必要がある. 以下, $\mathbb{R}$ の和と積を $+$ と $\cdot$ で, $\mathbb{C}$ の和と積を $+_{\mathbb{C}}$ と $\cdot_{\mathbb{C}}$ で, $\mathbb{R}^2$ の和と積を $+_{\mathbb{R}^2}$ と $\cdot_{\mathbb{R}^2}$ で書く. まず通常の複素数の和を考えると, 複素数 $x = a + b\sqrt{-1}$ と $y = c + d\sqrt{-1}$ ($a, b, c, d \in \mathbb{R}$) の和は $x +_{\mathbb{C}} y = (a + c) + (b + d)\sqrt{-1}$ である. したがって, $\mathbb{R}^2$ を複素数だと思うために, (a, b) と (c, d) の和は $(a, b) +_{\mathbb{R}^2} (c, d) = (a + c, b + d)$ と定義すればよい. では積を定義する.

- (a) $(\sqrt{-1}) \cdot_{\mathbb{C}} (\sqrt{-1}) = -1$ から $(0, 1) \cdot_{\mathbb{R}^2} (0, 1)$ の答えはどうなるか求めよ.
- (b) $(1 + 2\sqrt{-1}) \cdot_{\mathbb{C}} (2 - \sqrt{-1})$ と $(1, 2) \cdot_{\mathbb{R}^2} (2, -1)$ を計算せよ.
- (c) $(a + b\sqrt{-1}) \cdot_{\mathbb{C}} (c + d\sqrt{-1})$ を実部と虚部に分かれるように計算せよ.
- (d) $\mathbb{R}^2$ を $\mathbb{C}$ と同一視するために, $(a, b) \cdot_{\mathbb{R}^2} (c, d)$ をどう定義すればいいか答えよ.

3. 以下の推論を証明せよ.

$$(P \rightarrow \neg Q) \wedge (Q \vee R) \wedge P \Rightarrow R.$$

4. 全称命題と存在命題の否定を考える.

- (a) 命題「任意の自然数 x に対して $x^3 > 0$ である」の否定を述べ, その真偽を答えよ.
- (b) 命題 $\neg(\forall x(P(x)))$ と同値な命題を答えよ.
- (c) 命題「ある自然数 x に対して $x^2 \leq 4$ である」の否定を述べ, その真偽を答えよ.
- (d) 命題 $\neg(\exists x(P(x)))$ と同値な命題を答えよ.
- (e) 命題 $\neg(\forall x \exists y(P(x, y)))$ と同値な命題を答えよ.

5. $\{1, 2, 3\}$ を全体集合とする. 次の命題の真偽を述べよ.

- (a) $\forall x \forall y (x^2 + 2y < 10)$
- (b) $\exists x \exists y (x^2 + 2y < 10)$
- (c) $\exists x \forall y (x^2 + 2y < 10)$
- (d) $\forall x \exists y (x^2 + 2y < 10)$

6. 自然数 n に対して, $A_n = \{0, n\}$ とする. このとき, $\bigcap_{k=1}^{\infty} A_k$ と $\bigcup_{k=1}^{\infty} A_k$ をそれぞれ求めよ.

2 情報数理 A の復習 (写像)

2.1 写像

空集合でない集合 X から集合 Y への対応を考える. このとき次の 2 つの性質を持つとき, X から Y への写像 (map) と呼ぶ.

1. X の 1 つの要素から対応する Y の要素は 1 つしかない (X の異なる 2 つの要素が同じ Y の要素と対応してもよい).
2. 任意の X の要素について, 対応する Y の要素が必ずある.

一般に, 集合 X から集合 Y への写像を

$$f: X \rightarrow Y$$

と書く. これは写像 f によって, X の要素 x に対応して, Y の要素 $f(x)$ が定まっていることを意味している. また写像によって要素 x に対して要素 y が対応することを $x \mapsto y$ と書く. 上の f で考えると, $x \mapsto f(x)$ となっている. この記号は写像を具体的に定義するときによく使う.

写像 $f: X \rightarrow Y$ に対し, 集合 X を f の定義域と呼び, $\text{dom}(f)$ と書き, 集合 Y を f の終域と呼び, $\text{codom}(f)$ と書く. また要素 $x \in X$ に対応する Y の要素 $f(x)$ は f による x の像 (image) という. この像を全て集めた集合

$$\text{Im}(f) := \{f(x) : x \in X\}$$

を f の像という. このとき, いつでも $\text{Im}(f) \subset Y$ であるが, $\text{Im}(f) = Y$ になるとは限らない. また部分集合 $A \subset X$ に対し,

$$f(A) := \{f(x) : x \in A\}$$

を f による A の像という. このとき,

- $f(X) = \text{Im}(f)$ かつ $f(\emptyset) = \emptyset$
- $A_1 \subset A_2 \subset X$ ならば $f(A_1) \subset f(A_2) \subset f(X)$

が成り立つ. Y の部分集合 B に対し, 集合 $f^{-1}(B) \subset X$ を

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

で定義する. つまり f に対応する Y の要素が B に含まれる X の要素全体の集合である. これを f による B の逆像 (inverse image) という. ただし, $f^{-1}(\emptyset) = \emptyset$ としておく. この定義の中で, f^{-1} はただの記号で, 写像を表していないことに注意する. 実際, f^{-1} が f の逆対応とすると, f^{-1} は写像の条件 (1) または (2) を満たさないことがある.

2.2 全射と単射

写像 $f: X \rightarrow Y$ が全射 (surjective) または上への写像 (onto) であるとは, 任意の $y \in Y$ に対し, $y = f(x)$ を満たす $x \in X$ が存在するときという. つまり, どんな Y の要素も f によって対応があるということである. 論理式で書くと次の命題が真となる:

$$\forall y \in Y, \exists x \in X (y = f(x))$$

これは $\text{Im}(f) = Y$ と同値である. f が全射であることを $f: X \twoheadrightarrow Y$ で表す.

写像 $f: X \rightarrow Y$ が単射 (injective) または 1 対 1 (one-to-one) であるとは, 任意の 2 つの $x_1, x_2 \in X$ に対し, $x_1 \neq x_2$ ならば $f(x_1) \neq f(x_2)$ となるときという. つまり, X の各要素は, f によって異なる Y の要素に対応するということである. 論理式で書くと

$$\forall x_1, x_2 \in X (x_1 \neq x_2 \rightarrow f(x_1) \neq f(x_2))$$

が真となることである。対偶を考えれば、

$$\forall x_1, x_2 \in X (f(x_1) = f(x_2) \rightarrow x_1 = x_2)$$

である。つまり、 Y のある要素が f によって対応していれば、対応する X の要素はただ 1 つ（一意的）に定まるということである。 f が単射であることを $f: X \hookrightarrow Y$ で表す。

写像 $f: X \rightarrow Y$ が全射かつ単射であるとき、**全単射** (bijective) と呼ぶ。 f が全単射なとき、 f の逆対応を f^{-1} で表すと、これは写像の定義を満たす。この写像 f^{-1} は f の**逆写像**と呼ぶ。集合 A のある要素 a を同じ要素 a に対応させる写像 $\text{id}_A: A \rightarrow A, a \mapsto a$ のことを A の**恒等写像** (identity map) という。逆写像を正確に定義すると、写像 $f: X \rightarrow Y$ に対し、写像 $g: Y \rightarrow X$ で $g \circ f = \text{id}_X$ かつ $f \circ g = \text{id}_Y$ となるものを f の逆写像と呼び、 f^{-1} と書くのである。また写像 f が全単射になることと、 f が逆写像を持つことは同値である。

2.3 演習問題

1. 集合 X, Y を $X = \{1, 2, 3\}, Y = \{4, 5, 6\}$ により定め、写像 $f: X \rightarrow Y$ を $f(1) = 4, f(2) = 4, f(3) = 5$ で定義する。

(a) $f(\{1\}), f(\{1, 2\}), f(X)$ を求めよ。

(b) $f^{-1}(\{6\}), f^{-1}(\{4, 6\}), f^{-1}(\{4, 5\})$ を求めよ。

(c) f^{-1} を f の逆対応として定義したとき、 f^{-1} が写像とはならないことを説明せよ。

2. 写像 $f: X \rightarrow Y$ と X の部分集合 A_1, A_2 を考える。以下の文章を完成させて命題「 $A_1 \subset A_2$ ならば $f(A_1) \subset f(A_2)$ である」を証明せよ。

(証明) 集合 A_1, A_2 に対し、命題「 $A_1 \subset A_2$ 」を論理式で書くと、

$$\forall a \in A_1 (a \in A_2)$$

である。したがって、示したい命題を論理式で書くと

$$\forall a \in A_1 (a \in A_2) \rightarrow \boxed{} \quad (1)$$

である。この論理式が真であることを示すために、任意の $x \in f(A_1)$ をとる。すると集合 $\boxed{}$ のある元 a を使って $x = \boxed{}$ と書ける。このとき、 $A_1 \subset A_2$ より $a \in \boxed{}$ が成り立つ。よって $x \in \boxed{}$ が成り立ち、論理式 (1) が真であることがわかるので $f(A_1) \subset f(A_2)$ が従う。

3. 写像 $f: X \rightarrow Y$ と Y の部分集合 B_1, B_2 を考える。このとき、命題「 $B_1 \subset B_2$ ならば $f^{-1}(B_1) \subset f^{-1}(B_2)$ である」を証明せよ。

4. 写像 $f: \mathbb{R} \rightarrow \mathbb{R}$ を $x \mapsto x^2$ で定義する。

(a) f が全射でないことを示せ。

(b) f が単射でないことを示せ。

5. 非負の実数全体の集合を $\mathbb{R}_{\geq 0}$ と書き、写像 $f: \mathbb{R}_{\geq 0} \rightarrow \mathbb{R}_{\geq 0}$ を $x \mapsto x^2$ で定義する。

(a) f が全射であることを示せ。

(b) f が単射であることを示せ。

(c) f の逆写像 f^{-1} を求めよ。

3 二項関係

3.1 二項関係

東邦大学の学生の集合 X を、仮に

$$X = \{\text{フェルマー, オイラー, ガウス, セール, ヒルベルト, エルデシュ}\}$$

とし、東邦大学の学部集合を

$$Y = \{\text{医, 薬, 理, 看護, 健康科学}\}$$

とする。集合 X と集合 Y を個別に考えると、これらはただの独立した集合であるが、「学生」と「その学生が所属する学部」を考えると、2つの集合の要素の間に「関係」が現れる。例えば、「フェルマーは医」、「オイラーは看護」、「ガウスは理」、「セールは健康科学」、「ヒルベルトは薬」、「エルデシュは理」としよう。この「関係」というものを数学的に定義するにはどうすればいいか。上の「関係」は結局、 X の要素（学生） x と Y の要素（学部） y の組の集まりである。これは順序対 (x, y) を使って表すのがよさそうである。実際、直積集合 $X \times Y$ の部分集合 R を

$$R = \{(\text{フェルマー, 医}), (\text{オイラー, 看護}), (\text{ガウス, 理}), (\text{セール, 健康科学}), (\text{ヒルベルト, 薬}), (\text{エルデシュ, 理})\}$$

とすると、この集合 R は上の「関係」を完全に表していることが分かるであろう。これを踏まえて2つの集合の「関係」を定義する。

定義 3.1. X と Y を集合としたとき、直積集合 $X \times Y$ の部分集合 R を X から Y への**二項関係** (binary relation)、または単に**関係** (relation) と言う。つまり、 R が X から Y への二項関係であるとは、

$$R \subset X \times Y$$

であることである。特に、 $X = Y$ のとき、 R は X 上の**(二項) 関係**と呼ぶ。 $(x, y) \in R$ のことを xRy とも書く。またこのとき、 x と y は R 関係であるという。

例 3.2. 集合 $X = \{1, 2, 3\}$ に対し、

$$R = \{(1, 1), (1, 2), (1, 3), (2, 2), (2, 3), (3, 3)\}, \quad S = \{(1, 1), (2, 2), (3, 3)\}$$

とすると、 R と S は $X \times X$ の部分集合なので X 上の関係である。上の記法を使うと、 $1R2$ や $3S3$ が成り立つが、 R や S の代わりに「 $\leq$ 」と「 $=$ 」という記号を使うと、 $1 \leq 2$ と $3 = 3$ を意味していることがわかる。結局、 R は X 上の $\leq$ (以下) という関係を表し S は X 上の $=$ (等しい) という関係を表す。

例 3.3. 集合 X と Y に対し、空集合 $\emptyset$ は任意の集合の部分集合である、特に $\emptyset \subset X \times Y$ であるので、 $\emptyset$ は X から Y への関係となる。特にこれを**空関係** (empty relation) という。また $X \times Y$ 自身も $X \times Y$ の部分集合であるので、 $X \times Y$ は X から Y への関係となっている。特にこれを**全体関係** (total relation) という。

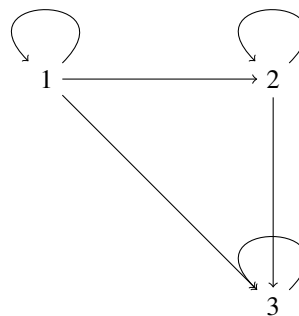
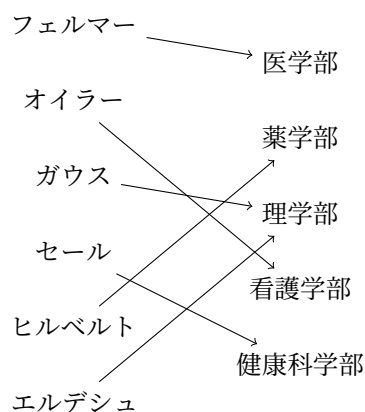
ここで、 $X = Y$ とし、次の X 上の関係を考える：

$$\text{Id}_X = \{(x, x) : x \in X\} = \{(x_1, x_2) \in X \times X : x_1 = x_2\}.$$

この関係を X の**恒等関係** (identity relation) という。

3.2 矢線図と有向グラフ

有限集合 X と Y が有限集合のとき、 X から Y への関係は**矢線図** (arrow diagram) を用いて表現することができる。例えば、前ページの「学生」と「学部」の関係の矢線図は以下の左図ようになる。また、集合 X 上の関係は矢線図の他に**有向グラフ** (directed graph または digraph) を用いて表現することもできる。例えば、例 3.2 の X 上の関係 R は以下の右図で表現される。



3.3 二項関係の演算

2つの X から Y への関係 R と S を考える. このとき, R と S は $X \times Y$ の部分集合であるので, その合併 $R \cup S$, 共通部分 $R \cap S$, 差 $R \setminus S$ は再び $X \times Y$ の部分集合となるので, これらも X から Y への関係である. つまり, X から Y への関係は, これら集合の演算で閉じていることがわかる.

例 3.4. $X = \{1, 2, 3\}$ を学生の集合, $Y = \{a, b, c\}$ を科目の集合とし, 次の X から Y への関係を考える.

- $R = \{(1, a), (2, b), (2, c), (3, b)\}$ は「学生」と「その学生が受講している科目」を表す関係,
- $S = \{(1, a), (1, b), (2, b), (3, c)\}$ は「学生」と「その学生が興味を持っている科目」を表す関係.

このとき,

- $R \cup S = \{(1, a), (1, b), (2, b), (2, c), (3, b), (3, c)\}$ は「学生」と「その学生が受講している, または興味を持っている科目」を表す関係,
- $R \cap S = \{(1, a), (2, b)\}$ は「学生」と「その学生が興味を持って受講している科目」を表す関係,
- $R \setminus S = \{(2, c), (3, b)\}$ は「学生」と「その学生が受講しているが興味のない科目」を表す関係

となっている.

集合 X から Y への関係 R に対し, その補集合

$$R^c = (X \times Y) \setminus R$$

は再び X から Y への関係であり, これを R の補関係 (complement relation) という. 例 3.4 において, $R^c = \{(1, b), (1, c), (2, a), (3, a), (3, c)\}$ は「学生」と「その学生が受講していない科目」を表す関係となる.

3.4 逆関係

R を X から Y への関係, つまり $R \subset X \times Y$ とする. このとき, R の逆関係 (inverse relation) R^{-1} は, $\{(y, x) \in Y \times X : (x, y) \in R\}$ で与えられる Y から X への関係である. 定義から $xRy \iff yR^{-1}x$ が従う.

例 3.5. 例 3.4 の集合と関係を考えて,

- $R^{-1} = \{(a, 1), (b, 2), (c, 2), (b, 3)\}$ は「科目」と「その科目を受講している学生」を表す関係,
- $S^{-1} = \{(a, 1), (b, 1), (b, 2), (c, 3)\}$ は「科目」と「その科目に興味を持っている学生」を表す関係

となっている.

命題 3.6. R と S を集合 X から集合 Y への関係とする。このとき、次が成り立つ：

1. $(R^{-1})^{-1} = R$.
2. $R \subset S$ ならば $R^{-1} \subset S^{-1}$
3. $(R \cup S)^{-1} = R^{-1} \cup S^{-1}$
4. $(R \cap S)^{-1} = R^{-1} \cap S^{-1}$

Proof. 簡単な演習問題なので、(3) のみを証明する。二つの集合が $A = B$ であることを証明する手法（定義）の一つは $A \subset B$ と $B \subset A$ の両方を証明することである。

まず $(R \cup S)^{-1} \subset R^{-1} \cup S^{-1}$ を示す。ここで $(R \cup S)^{-1}$ と $R^{-1} \cup S^{-1}$ は Y から X への関係であることに注意する。任意の $(y, x) \in (R \cup S)^{-1}$ をとると、このとき、逆関係の定義から $(x, y) \in R \cup S$ である。つまり $(x, y) \in R$ または $(x, y) \in S$ である。これは、再び逆関係の定義から、 $(y, x) \in R^{-1}$ または $(y, x) \in S^{-1}$ を意味するので、 $(y, x) \in R^{-1} \cup S^{-1}$ が従う。よって $(R \cup S)^{-1} \subset R^{-1} \cup S^{-1}$ となる。

次に、 $R^{-1} \cup S^{-1} \subset (R \cup S)^{-1}$ を示す。任意の $(y, x) \in R^{-1} \cup S^{-1}$ をとると、これは $(y, x) \in R^{-1}$ または $(y, x) \in S^{-1}$ を意味する。逆関係の定義より、 $(x, y) \in R$ または $(x, y) \in S$ が従い、つまり $(x, y) \in R \cup S$ となる。このとき、再び逆関係の定義から、 $(y, x) \in (R \cup S)^{-1}$ が従う。よって $R^{-1} \cup S^{-1} \subset (R \cup S)^{-1}$ となる。

以上から $(R \cup S)^{-1} = R^{-1} \cup S^{-1}$ が証明できた。 $\square$

3.5 合成関係

集合 X から Y への二項関係 R と集合 Y から Z への関係 S を考える。このとき、 X から Z への関係 $R \circ S$ （これで一つの関係を表す）を

$$S \circ R = \{(x, z) \in X \times Z : \text{ある } y \in Y \text{ に対して } xRy \text{ かつ } ySz \text{ である}\}$$

により定めることができる。すなわち、

$$S \circ R = \{(x, z) \in X \times Z : \exists y \in Y ((x, y) \in R \wedge (y, z) \in S)\}$$

である。これを R と S の**合成関係** (composite relation) という。 R と S の順番を間違えないように注意！

例 3.7. $X = \{1, 2, 3\}$ を学生の集合 $Y = \{a, b, c, d\}$ を科目の集合、 $Z = \{\alpha, \beta, \gamma\}$ を先生の集合とし、

- $R = \{(1, a), (2, b), (2, c), (3, b), (3, c), (3, d)\}$ を「学生」と「その学生が受講している科目」を表す関係、
- $S = \{(a, \alpha), (b, \beta), (b, \gamma), (c, \gamma), (d, \gamma)\}$ を「科目」と「その科目を担当している先生」を表す関係

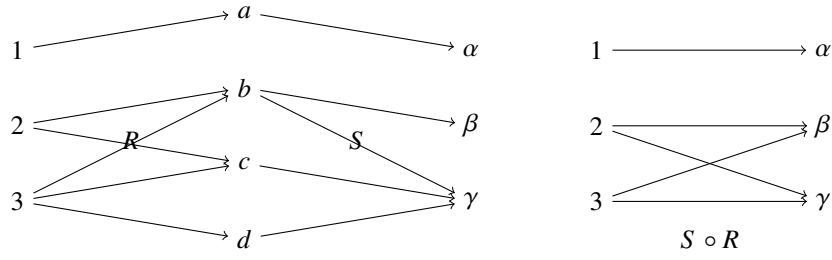
とすると、

$$S \circ R = \{(1, \alpha), (2, \beta), (2, \gamma), (3, \beta), (3, \gamma)\}$$

は「学生」と「その学生の受講科目を担当している先生」を表す関係となる。矢線図で見ると、 R と S の矢線図を繋げて書いたとき、2つの矢印を通り辿り着ける2点を矢印で繋いだものが $S \circ R$ の矢線図である。

命題 3.8. 集合 X から Y への関係を R 、集合 Y から Z への関係を S 、集合 Z から W への関係を T とする。このとき、次が成り立つ。

1. $(S \circ R)^{-1} = R^{-1} \circ S^{-1}$,
2. $T \circ (S \circ R) = (T \circ S) \circ R$ (関係の合成に関する結合則),
3. $R \circ \text{Id}_X = R$ かつ $\text{Id}_Y \circ R = R$.



Proof. (1) $(z, x) \in Z \times X$ とすると, このとき,

$$\begin{aligned}
 (z, x) \in (S \circ R)^{-1} &\iff (x, z) \in S \circ R && \text{(逆関係の定義)} \\
 &\iff \exists y \in Y((x, y) \in R \wedge (y, z) \in S) && \text{(合成関係の定義)} \\
 &\iff \exists y \in Y((y, x) \in R^{-1} \wedge (z, y) \in S^{-1}) && \text{(逆関係の定義)} \\
 &\iff \exists y \in Y((z, y) \in S^{-1} \wedge (y, x) \in R^{-1}) && \text{(論理の交換律)} \\
 &\iff (z, x) \in R^{-1} \circ S^{-1} && \text{(合成関係の定義)}
 \end{aligned}$$

よって $(S \circ R)^{-1} = R^{-1} \circ S^{-1}$ である.

(2) 次の事実に注意する.

$$\exists x P(x) \wedge Q \iff \exists x (P(x) \wedge Q) \quad (*)$$

$$\exists x \exists y P(x, y) \iff \exists y \exists x P(x, y) \quad (**)$$

$(x, w) \in X \times W$ とすると, このとき,

$$\begin{aligned}
 (x, w) \in T \circ (S \circ R) &\iff \exists z \in Z(\underline{(x, z) \in S \circ R} \wedge (z, w) \in T) && \text{(合成関係の定義)} \\
 &\iff \exists z \in Z(\underline{(\exists y \in Y((x, y) \in R \wedge (y, z) \in S))} \wedge (z, w) \in T) && \text{(合成関係の定義)} \\
 &\iff \exists z \in Z(\underline{\exists y \in Y(((x, y) \in R \wedge (y, z) \in S) \wedge (z, w) \in T)}) && (*) \\
 &\iff \underline{\exists z \in Z \exists y \in Y((x, y) \in R \wedge (y, z) \in S \wedge (z, w) \in T)} && \text{(論理の結合律)} \\
 &\iff \exists y \in Y \underline{\exists z \in Z((x, y) \in R \wedge (y, z) \in S \wedge (z, w) \in T)} && (**) \\
 &\iff \exists y \in Y((x, y) \in R \wedge \underline{\exists z \in Z((y, z) \in S \wedge (z, w) \in T)}) && (*) \\
 &\iff \exists y \in Y((x, y) \in R \wedge (y, w) \in T \circ S) && \text{(合成関係の定義)} \\
 &\iff (x, w) \in (T \circ S) \circ R && \text{(合成関係の定義)}
 \end{aligned}$$

よって $T \circ (S \circ R) = (T \circ S) \circ R$ である.

(3) $(x, y) \in X \times Y$ とすると, このとき,

$$\begin{aligned}
 (x, y) \in R \circ \text{Id}_X &\iff \exists x' \in X((x, x') \in \text{Id}_X \wedge (x', y) \in R) && \text{(合成関係の定義)} \\
 &\iff \exists x' \in X(x = x' \wedge (x', y) \in R) && \text{(恒等関係の定義)} \\
 &\iff (x, y) \in R
 \end{aligned}$$

よって $R \circ \text{Id}_X = R$ である. $\text{Id}_Y \circ R = R$ も同様.

□

4 同値関係

直積集合 $X \times Y$ の部分集合のことを、 X から Y への（二項）関係、特に、 $X = Y$ のときは、 X 上の（二項）関係と呼んでいた。本節では特別な X 上の関係を考えることで、集合 X における「等しい（＝）」という概念を拡張する。

4.1 反射的な関係

定義 4.1. 集合 X 上の関係 R が**反射的** (reflexive) であるとは、任意の $x \in X$ に対して $(x, x) \in R$ であるときにいう。つまり、

$$R \text{ が反射的である} \iff \forall x \in X ((x, x) \in R) \iff \text{Id}_X \subset R$$

である。ここで、 Id_X は X の恒等関係である。

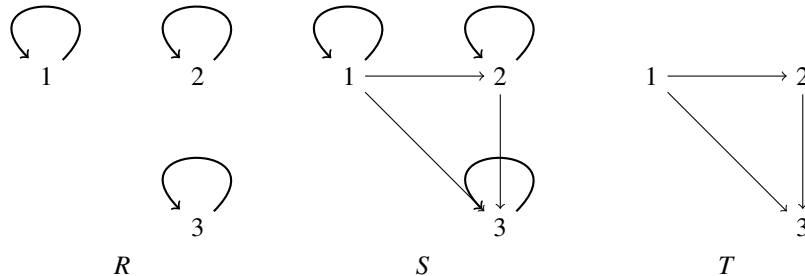
例 4.2. $X = \{1, 2, 3\}$ とし、 X 上の関係

$$R = \{(1, 1), (2, 2), (3, 3)\}$$

$$S = \{(1, 1), (1, 2), (1, 3), (2, 2), (2, 3), (3, 3)\}$$

$$T = \{(1, 2), (1, 3), (2, 3)\}$$

を考える。 R, S, T はそれぞれ、 $=, \leq, <$ という関係を表していることに注意する。特に、 R は X の恒等関係 Id_X に他ならない。反射律の 3 つ目の同値条件を考えると、 $\text{Id}_X \subset \text{Id}_X$ なので、 R は反射的である。また $R \subset S$ なので、 S も反射的である。一般に、反射的な関係を部分集合に持つ関係は、再び反射的となる。最後に T を考えると、 $1 \in X$ に対して、 $(1, 1) \notin T$ なので、 T は反射的ではない。有向グラフで考えると、反射的な関係とは、全ての頂点にループ辺が存在する関係のことである。



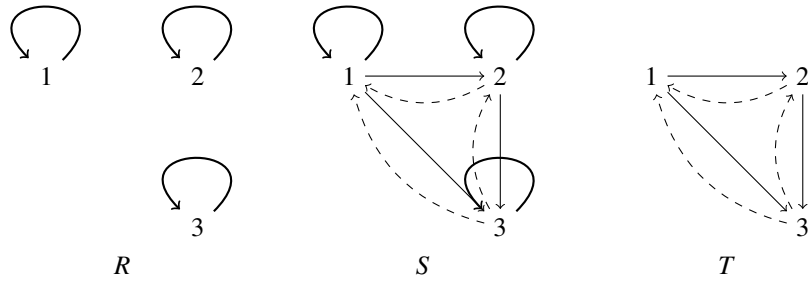
4.2 対称的な関係

定義 4.3. 集合 X 上の関係 R が**対称的** (symmetric) であるとは、任意の $a, b \in X$ に対して $(a, b) \in R$ ならばいつでも $(b, a) \in R$ であるときにいう。つまり、

$$R \text{ が対称的である} \iff \forall a, b \in X ((a, b) \in R \rightarrow (b, a) \in R) \iff R = R^{-1}.$$

ここで、 R^{-1} は R の逆関係である。

例 4.4. 例 4.2 の集合 X と X 上の関係 R, S, T を考える。任意の集合 A に対して、 $(\text{Id}_A)^{-1} = \text{Id}_A$ であるので、 R は対称的である。一方、 $1, 2 \in X$ に対し、 $(1, 2) \in S$ （同様に $(1, 2) \in T$ ）であるが、 $(2, 1) \notin S$ （同様に $(2, 1) \notin T$ ）であるので、 S および T は対称的ではない。有向グラフで見ると、対称的な関係とは、ある頂点から頂点への矢印があれば、必ず逆方向の矢印も存在する関係である。ただし、ループ辺は自分自身が逆方向の矢印となる。



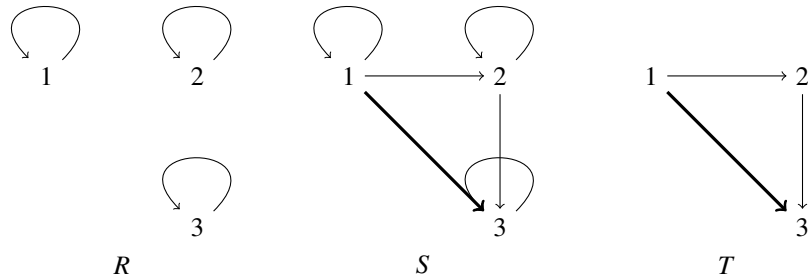
4.3 推移的な関係

定義 4.5. 集合 X 上の関係 R が**推移的** (transitive) であるとは、任意の $a, b, c \in X$ に対して、 $(a, b) \in R$ かつ $(b, c) \in R$ ならばいつでも $(a, c) \in R$ となるときをいう。つまり、

$$R \text{ が推移的である} \iff \forall a, b, c \in X ((aRb \wedge bRc) \rightarrow aRc) \iff R \circ R \subset R.$$

ここで、 $R \circ R$ は R と R の合成関係である。

例 4.6. 例 4.2 の集合 X と X 上の関係 R, S, T を考える。任意の集合 A に対して、 $\text{Id}_A \circ \text{Id}_A = \text{Id}_A \subset \text{Id}_A$ であるので、 R は推移的である。一方、簡単な計算により、 $S \circ S = S$ と $T \circ T = \{(1, 3)\} \subset T$ がわかるので、 S も T も推移的となる。有向グラフで考えると、推移的な関係とは、ある 2 頂点が 2 つの矢印を通り辿り着けるなら、その 2 点間に近道となる矢印が必ずあるということである。



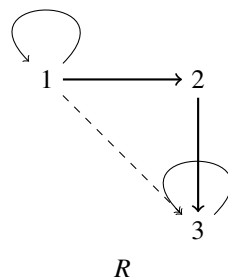
例 4.7. 推移的でない二項関係の例も見ておこう。 $X = \{1, 2, 3\}$ とし、 X 上の二項関係を

$$R = \{(1, 1), (1, 2), (2, 3), (3, 3)\}$$

とすると、 $(1, 2), (2, 3) \in R$ だが、 $(1, 3) \notin R$ なので、 R は推移的ではない。特に、

$$R \circ R = \{(1, 1), (1, 2), (1, 3), (2, 3), (3, 3)\}$$

なので $R \circ R \not\subset R$ である。有向グラフで考えると、1 と 3 は 2 本の矢印を通り辿り着けるが、その間には近道がない。



4.4 同値関係

定義 4.8. 集合 X 上の関係 R が**同値関係** (equivalence relation) であるとは、 R が反射的かつ対称的かつ推移的であるときにいう。この3つの条件をそれぞれ**反射律**、**対称律**、**推移律**という。 R が同値関係のとき、 aRb ならば、 a と b は R に関して**同値**であるという。同値関係には $\sim$ や $\equiv$ という記号がよく使われる。このとき、 a と b が同値ではないとき、 $a \nabla b$ や $a \not\equiv b$ と書く。

同値関係は「なんらかの意味で等しい」を意味する関係であり、これまでの「等しい (=)」という概念を拡張している。まず「等しい (=)」が実際に同値関係であることを確認する。

例 4.9. 例 4.2 の集合 X と X 上の関係 R, S, T を考える。これまでの結果をまとめると、以下の表が成り立つ：

関係	反射律	対称律	推移律	同値関係
R	○	○	○	○
S	○	×	○	×
T	×	×	○	×

R, S, T はそれぞれ、 $=, \leq, <$ という関係を表していたことを思い出そう。同値関係は「等しい」という概念を拡張したものなので、 $=$ だけが同値関係となるのは納得できるであろう。

次に、「なんらかの意味で等しい」ということを具体例で確認してみる。

例 4.10. この教室にいる学生の集合を X とする。今、 X 上の二項関係 $\sim$ を

$$\sim = \{(a, b) \in X^2 : a \text{ と } b \text{ の誕生月が同じである}\}$$

で定義する。ただし、自分自身とも誕生月が同じであるとみなすことに注意する。これは反射律が成り立つことを意味する。また a と b の誕生月が同じであればもちろん b と a の誕生月も同じなので、対称律も成り立つ。最後に、 a と b の誕生月が同じでかつ b と c の誕生月が同じであれば、 a と c の誕生月も同じであるので、推移律も成り立つ。以上より、 $\sim$ は同値関係となる。

注意 4.11. 例 4.10 のように、順序対 (a, b) に同じ法則で二項関係を定義するとき、集合の形ではなく、次のような書き方をすることがある。「 X 上の二項関係 $\sim$ を

$$a \sim b \iff a \text{ と } b \text{ の誕生月が同じである}$$

で定義する」こちらの方が、上の集合の形で定義するよりわかりやすいだろう。意味は同じなので、どっちで書かれていても理解できるようにしよう。

次に、似たように定義した2つの二項関係が、片方は同値関係になり、もう片方はならない場合があることを見る。

例 4.12. $\mathbb{Z}$ 上の二項関係、 $\sim_E$ と $\sim_O$ を

$$a \sim_E b \iff a - b \text{ が偶数}$$

$$a \sim_O b \iff a - b \text{ が奇数}$$

で定義する。後で証明する命題 4.15 を使うと $\sim_E$ は同値関係となる。一方、 $\sim_O$ は同値関係ではない。実際、 $1 \in \mathbb{Z}$ に対し、 $1 - 1 = 0$ は奇数ではないので、 $1 \not\sim_O 1$ であり、反射律が成り立たない。また推移律も成り立たない。似たような定義でも同値関係になるかどうかはわからない。この2つの二項関係にはどういった差があるのか、なぜ同値関係の定義に3つの性質を必要とするのか。その理由は集合を「なんらかの意味で等しいもの」で**グループ分け**したいからである。これは次回説明する。

任意の集合 X に対して、恒等関係 Id_X はいつでも同値関係であった。これとは別に、明らかに同値関係となるものももう一つある。

例 4.13. 集合 X に対し、全体関係 $X \times X$ は同値関係である。この同値関係は集合の要素が全て「等しい」ということになる。この同値関係を X の**自明な同値関係**と呼ぶ。

4.5 合同式

同値関係の代表例の1つは整数に対する合同式である。

定義 4.14. 自然数 m に対し、整数 a と b が m を**法 (module)** として**合同 (congruent)** であるとは、 $a - b$ が m の倍数となるときにいう。このとき、

$$a \equiv_m b \text{ または } a \equiv b \pmod{m}$$

と書く。法 m が文脈から明らかときは、単に $a \equiv b$ と書くこともある。

例えば、 $5 \equiv_3 2 \equiv_3 -1$ であり、これは3で割った余りが等しいという関係を表す。これは高校数学の発展として教科書に書かれている。この合同式 $\equiv_m$ が実は同値関係であることを示そう。そのために、 $\equiv_m$ を $\mathbb{Z}$ 上の二項関係で再定義する。自然数 m に対して、 $m\mathbb{Z} = \{mx : x \in \mathbb{Z}\}$ 、つまり m の倍数全体の集合とすると、合同式は $\mathbb{Z}$ 上の二項関係として

$$a \equiv_m b \iff a - b \in m\mathbb{Z}$$

で定義できる。例えば、 $5 - 2 = 3 = 3 \cdot 1 \in 3\mathbb{Z}$ なので、 $5 \equiv_3 2$ である。

命題 4.15. m を自然数とする。 $\mathbb{Z}$ 上の二項関係 $\equiv_m$ は同値関係である。

Proof. (反射律) 任意の整数 $a \in \mathbb{Z}$ に対し、 $a - a = 0 = m \cdot 0 \in m\mathbb{Z}$ なので、 $a \equiv_m a$ が従い、 $\equiv_m$ は反射的である。

(対称律) 任意の整数 $a, b \in \mathbb{Z}$ で、 $a \equiv_m b$ となるものをとってくる。このとき、 $a - b \in m\mathbb{Z}$ であるので、ある整数 k に対し、 $a - b = mk$ と書ける。 $b - a = -mk = m(-k)$ であり、 $-k$ は整数なので、 $b - a \in m\mathbb{Z}$ が従う。よって $b \equiv_m a$ となり、 $\equiv_m$ は対称的である。

(推移律) 任意の整数 $a, b, c \in \mathbb{Z}$ で、 $a \equiv_m b$ かつ $b \equiv_m c$ となるものをとってくる。このとき、 $a - b, b - c \in m\mathbb{Z}$ なので、ある整数 k と ℓ に対し、 $a - b = mk, b - c = m\ell$ と書ける。

$$a - c = (a - b) + (b - c) = mk + m\ell = m(k + \ell)$$

となり、 $k + \ell$ は整数であるので、 $a - c \in m\mathbb{Z}$ が従う。よって $a \equiv_m c$ となり、 $\equiv_m$ は推移的である。

以上より、 $\equiv_m$ は反射律、対称律、推移律が成り立つので、同値関係である。 $\square$

合同式の定義において、「 $a - b \in m\mathbb{Z}$ 」というのは「 $a - b$ が m で割り切れる」を意味する。高校数学で1変数多項式の割り算を勉強したと思うが、その場合にも合同式は定義できる。今、 x を変数とする実数を係数に持つ多項式全体の集合を $\mathbb{R}[x]$ と書く。例えば、 $x^2 + 1 \in \mathbb{R}[x]$ である。ゼロでない多項式 $p \in \mathbb{R}[x]$ に対し、 $\mathbb{R}[x]$ 上の二項関係を

$$f \equiv_p g \iff f - g \text{ は } p \text{ で割り切れる}$$

で定義する。このとき $\equiv_p$ は同値関係となる。例えば、 $p = x^2 + 1$ とすると、 $x^3 \equiv_p -x$ である。同値関係であることの証明は、 $f - g$ が p で割り切れるということが、ある多項式 $q \in \mathbb{R}[x]$ に対して、 $f - g = pq$ と書けることを意味することに注意すれば、命題 4.15 と同様にできる。代数学をさらに学んでいくと、 $\mathbb{Z}$ や $\mathbb{R}[x]$ の合同式は「**環 (ring)**」の「**イデアル (ideal)**」という概念に拡張される ($\mathbb{Z}$ や $\mathbb{R}[x]$ は整数環や1変数多項式環と呼ばれ、環の一種である)。環やイデアルは整数や多項式などを統一的に扱うための代数学において基本的かつ極めて重要な概念であり、数理コース3年の秋学期の情報代数学という授業で学ぶ。

5 同値類と商集合

集合 X 上の二項関係 R は反射律, 対称律, 推移律の3つを満たすとき, **同値関係**と呼んでいた. 同値関係は「なんらかの意味で等しい」を意味する関係であった. 同値関係のこの3つの性質は, 集合をこの「なんらかの意味で等しい」もので**分割**するために必要な性質である.

5.1 集合の分割

定義 5.1. 空でない集合 X の**分割** (partition) とは, X の部分集合族 $P \subset 2^X$ で条件

1. $\emptyset \notin P$
2. 任意の $x \in X$ に対して, $x \in A$ となる $A \in P$ が存在する
3. 任意の $A, B \in P$ に対して, $A \neq B$ ならば $A \cap B = \emptyset$

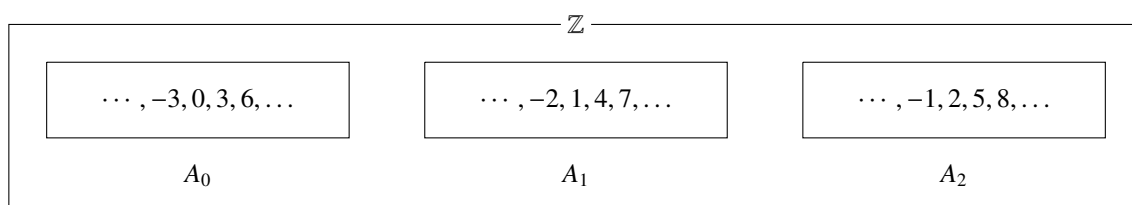
を満たすときにいう. P の元を分割の**ブロック** (block) という.

注意 5.2. (2) の条件は任意の $x \in X$ に対し, $x \in \bigcup_{A \in P} A$ が成り立つことを意味し, これは $X = \bigcup_{A \in P} A$ と同値である. また2つの集合 A と B が**互いに素**とは, $A \cap B = \emptyset$ を満たすときにいい, $A \cap B \neq \emptyset$ を満たすときは, **交わる**という. つまり条件 (3) は P の相異なる元は互いに素ということになる.

例 5.3. 整数 $0 \leq r \leq 2$ に対し, 整数全体の集合 $\mathbb{Z}$ の部分集合 A_r を

$$A_r = \{a \in \mathbb{Z} : a \text{ を } 3 \text{ で割った余りが } r\}$$

と定義し, $P = \{A_0, A_1, A_2\}$ とする. ここで, a を3で割った余りとは, 整数 k と整数 $0 \leq \ell \leq 2$ を用いて $a = 3k + \ell$ と表したときの ℓ のことである. $0 \in A_0, 1 \in A_1, 2 \in A_2$ より $\emptyset \notin P$ から条件 (1) が成り立つ. また, 任意の $x \in \mathbb{Z}$ に対し, ある整数 k が存在して $x = 3k$ または $x = 3k + 1$ または $x = 3k + 2$ が成り立つが, $x = 3k$ ならば $x \in A_0$, $x = 3k + 1$ ならば $x \in A_1$, $x = 3k + 2$ ならば $x \in A_2$ となるので条件 (2) が成り立つ. 最後に, $A_0 \cap A_1 = \emptyset, A_0 \cap A_2 = \emptyset, A_1 \cap A_2 = \emptyset$ であるので条件 (3) が成り立つ. 以上より P は $\mathbb{Z}$ の分割である.



5.2 同値類と商集合

集合の分割は同値関係から構成することができる. そのために**同値類**と**商集合**という概念を導入する.

定義 5.4. $\sim$ を集合 X 上の同値関係とする. 各 $x \in X$ に対して, x と同値となる元全体の集合 $\{y \in X : x \sim y\}$ を x の $\sim$ による**同値類** (equivalent class) といい, $[x]_{\sim}$ や単に $[x]$ で表す. このとき, x は $[x]_{\sim}$ の**代表元** (representative element) という. さらに $\sim$ の同値類全体の集合 $\{[x]_{\sim} : x \in X\}$ を X の $\sim$ による**商集合** (quotient set) といい, $X/\sim$ で表す. また X の部分集合 S が $X/\sim$ の各元 (同値類) の代表元をちょうど1つずつ含むとき, S を $\sim$ の**完全代表系** (complete set of representative elements) と呼ぶ.

同値類は「なんらかの意味で等しい」ものの集まりであり, 商集合はその集まりごとの集合である. 例を見て考えてみよう.

例 5.5. 集合 $X = \{a, b, c, d, e\}$ 上の二項関係

$$R = \{(a, a), (b, b), (c, c), (d, d), (e, e), (a, e), (e, a), (b, c), (c, b)\}$$

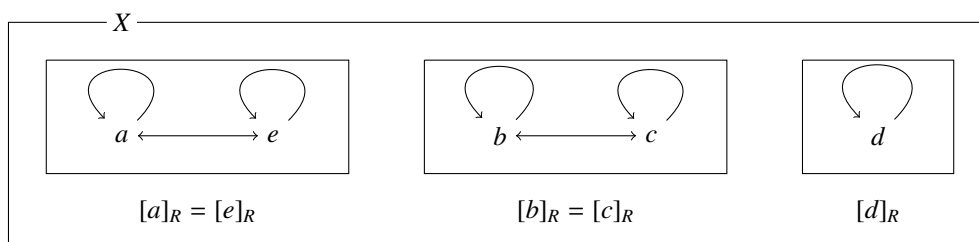
を考える. これが同値関係となっていることの確認は各自で行おう. このとき, R の同値類は

$$[a]_R = [e]_R = \{a, e\}, [b]_R = [c]_R = \{b, c\}, [d]_R = \{d\}$$

である. よって A の R による商集合は

$$X/R = \{[a]_R, [b]_R, [c]_R, [d]_R, [e]_R\} = \{[a]_R, [b]_R, [d]_R\} = \{\{a, e\}, \{b, c\}, \{d\}\}$$

となる. この商集合 X/R が X の分割になっていることも簡単に確認できる. また集合 $\{a, b, d\} \subset X$ は同値関係 R の完全代表系である. 完全代表系は一意に定まるとは限らず, 例えば $\{a, c, d\}$ も R の完全代表系である. この同値類や商集合は元の集合が有限集合であれば有向グラフを書いて想像しやすい. 実際, 同値関係 R に対応する有向グラフは



であり, いくつかの繋がっている島に分かれている. この各島のことを**連結成分** (connected component) と呼ぶ. 同値関係の有向グラフは各連結成分が自明な同値関係を表しており, それぞれが R の同値類と対応している. そして商集合はこの連結成分の集合とみなすことができる. さらに, 各頂点はそれぞれの連結成分が表す同値類の代表元であり, 各連結成分から 1 つずつ頂点をとったものが完全代表系である.

注意 5.6. $\sim$ を集合 X 上の同値関係とすると, 任意の $a, b \in X$ に対し,

$$a \sim b \Leftrightarrow [a] = [b]$$

が成り立つ. これは同値関係が対称的であることから従う (証明略).

例 5.7. 前回定義した自然数 m を法とした $\mathbb{Z}$ 上の合同式

$$a \equiv_m b \Leftrightarrow a - b \in m\mathbb{Z}$$

を考える. ここで, $m\mathbb{Z} = \{mx : x \in \mathbb{Z}\}$ である. この合同式は同値関係であった. 簡単のため $m = 3$ とし, 単に $\equiv$ と書く. 例えば, $5 \equiv 2$ であるので, $[5]_{\equiv} = [2]_{\equiv}$ であるが, この同値類を正確に求めるとどういった集合となるのだろうか. また商集合はどのようなものか. 実際, 例 5.3 で考えた集合 A_0, A_1, A_2 を考えると, $[2]_{\equiv} = A_2$ である. なぜなら任意の整数 $a \in A_2$ は $a = 3k + 2$ (k は整数) と表せ, $a - 2 = (3k + 2) - 2 = 3k \in 3\mathbb{Z}$, つまり $a \equiv 2$ であるので $a \in [2]_{\equiv}$ である. これは $A_2 \subset [2]_{\equiv}$ を意味する. 逆に任意の整数 $a \in [2]_{\equiv}$ をとると, $a - 2 \in 3\mathbb{Z}$ なので, $a - 2 = 3k$ (k は整数) と表せ, $a = 3k + 2$ からこれは $a \in A_2$ となる. つまり $[2]_{\equiv} \subset A_2$ となり, 結局 $[2]_{\equiv} = A_2$ となる. 同様に, $[1]_{\equiv} = A_1$ と $[0]_{\equiv} = A_0$ も証明できる. またどの整数も A_0, A_1, A_2 のいずれかの元なので, 商集合は

$$\mathbb{Z}/\equiv = \{[x]_{\equiv} : x \in \mathbb{Z}\} = \{A_0, A_1, A_2\}$$

となる. さらに集合 $\{1, 2, 3\} \subset \mathbb{Z}$ は合同式 $\equiv$ の完全代表系である.

5.3 同値関係と分割

例で見た通り、ここでどんな同値関係に対しても商集合が分割となっていることを示そう。

命題 5.8. $\sim$ を集合 X 上の同値関係とする。商集合 $X/\sim$ は X の分割である。

Proof. (1) 勝手な同値類 $[x] \in X/\sim$ をとる。ただし $x \in X$ である。 $\sim$ は同値関係なので反射的であり、 $x \sim x$ だから、 $x \in [x]$ である。ゆえに $[x] \neq \emptyset$ である。よって $\emptyset \notin X/\sim$ となる。

(2) 任意の $x \in X$ に対して、 $A = [x] \in X/\sim$ とすれば、 $\sim$ の反射性より $x \sim x$ となり、 $x \in A \in X/\sim$ である。

(3) 任意の $A, B \in X/\sim$ をとる。対偶を証明するために $A \cap B \neq \emptyset$ を仮定する。 $X/\sim$ の定義から、ある $a \in X$ と $b \in X$ に対して、 $A = [a]$ と $B = [b]$ と書ける。 $A \cap B \neq \emptyset$ から、ある $c \in X$ で $c \in A$ かつ $c \in B$ を満たすものが存在する。つまり $c \in [a]$ かつ $c \in [b]$ である。同値類の定義からこれは $a \sim c$ かつ $b \sim c$ を意味する。 $\sim$ は対称的なので $c \sim b$ も成り立つ。さらに $\sim$ は推移的であるので、 $a \sim c$ かつ $c \sim b$ から $a \sim b$ が従う。よって $[a] = [b]$ 、つまり $A = B$ となる。対偶を考えると、結局 $A \neq B$ ならば $A \cap B = \emptyset$ が成り立つ。

以上より $X/\sim$ は X の分割である。 $\square$

この命題から集合 X の同値関係を 1 つ与えると、それに対応した X の分割が 1 つ得られることがわかった。逆に X の分割を 1 つ与えると、それに対応した同値関係も得ることができる。

命題 5.9. 集合 X とその分割 P に対し、 X 上の関係 $\sim$ を以下のように定義する：

$$a \sim b \Leftrightarrow a \in A \text{ かつ } b \in A \text{ を満たすブロック } A \in P \text{ が存在する.}$$

このとき、 $\sim$ は同値関係である。

Proof. (反射律) P は X の分割なので、分割の定義 (2) から任意の $a \in X$ に対し、 $a \in A$ となる $A \in P$ が存在する。したがって $\sim$ の定義から $a \sim a$ 、つまり $\sim$ は反射的である。

(対称律) 任意の $a, b \in X$ で $a \sim b$ となるものをとる。このとき、 $\sim$ の定義から、 $a \in A$ かつ $b \in A$ を満たす $A \in P$ が存在する。つまりある $A \in P$ に対し、 $b \in A$ かつ $a \in A$ となるので、 $b \sim a$ が成り立ち、 $\sim$ は対称的である。

(推移律) 任意の $a, b, c \in X$ で $a \sim b$ かつ $b \sim c$ となるものをとる。このとき、 $\sim$ の定義から、ある $A \in P$ に対し、 $a \in A$ かつ $b \in A$ 、さらにある $B \in P$ に対し、 $b \in B$ かつ $c \in B$ が成り立つ。 $b \in A$ かつ $b \in B$ より、 $b \in A \cap B$ が成り立ち、特に $A \cap B \neq \emptyset$ である。分割の定義 (3) の対偶を考えると、 $A = B$ が従う。よって $a \in A$ かつ $c \in A$ となり、 $a \sim c$ が成り立ち、 $\sim$ は推移的である。

以上より、 $\sim$ は同値関係である。 $\square$

この 2 つの命題から集合 X の同値関係を与えることと、分割を与えることは同じ操作であることがわかる。この分割を与えるという目的のため、同値関係の定義の 3 つの性質が必要となる。

5.4 一般角

高校数学で一般角を考えたとき、 2π (ラジアン) の整数倍だけ違うものは同じ角度であると見なす (同一視する) と便利なきががあった。実際、角度 θ と整数 n に対し、

$$\sin \theta = \sin(2n\pi + \theta), \quad \cos \theta = \cos(2n\pi + \theta)$$

が成り立つ。このように何かと何かを同一視するときに同値類が使われる。実数の集合 $\mathbb{R}$ 上の二項関係を

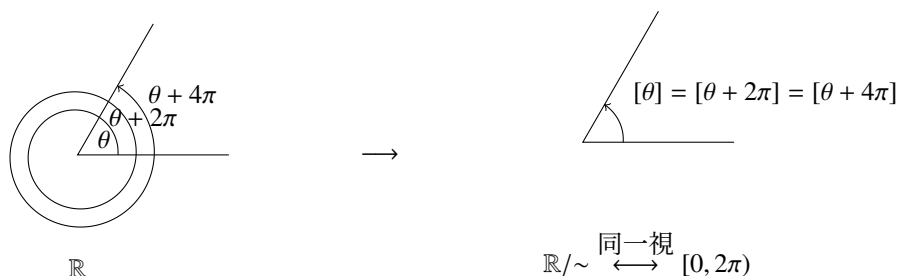
$$x \sim y \Leftrightarrow x - y \in \{2n\pi : n \in \mathbb{Z}\}$$

で定義する。この関係が同値関係となることの証明は演習問題とする。このとき、部分集合 $[0, 2\pi) = \{\theta \in \mathbb{R} : 0 \leq \theta < 2\pi\} \subset \mathbb{R}$ は同値関係 $\sim$ の完全代表系である。これを確かめるためには次の 2 つを示せばよい。

1. 任意の $x, y \in [0, 2\pi)$ に対し, $x \neq y$ ならば $[x] \neq [y]$ である.
2. 任意の $x \in \mathbb{R}$ に対し, ある $y \in [0, 2\pi)$ が存在して, $x \in [y]$ である.

Proof. (1) 任意の $x, y \in [0, 2\pi)$ に対し $x > y$ とすると $0 < x - y < 2\pi$ である. これは $x \neq y$ を意味する. 特に, $[x] \neq [y]$ である. (2) 任意の $x \in \mathbb{R}$ に対し, ある整数 n で $2n\pi \leq x < (2n+2)\pi$ となるものが存在する. $y = x - 2n\pi$ とすると, $0 \leq y < 2\pi$ が成り立つ. このとき, $x - y = 2n\pi$ となるので, $x \sim y$ である. よってこの y に対し, $x \in [y]$ が成り立つ. $\square$

今, 実数の集合 $\mathbb{R}$ を一般角全体の集合だと認識しよう. すると商集合 $\mathbb{R}/\sim$ と完全代表系 $[0, 2\pi)$ を同一視することで, 一般角 $\theta \in \mathbb{R}$ の $\sim$ による同値類 $[\theta] \in \mathbb{R}/\sim$ は一周内の角度と見なすことができる.



上記の $\sin$ と $\cos$ の一般角に関する式を商集合の言葉で書くと, 以下のようになる:

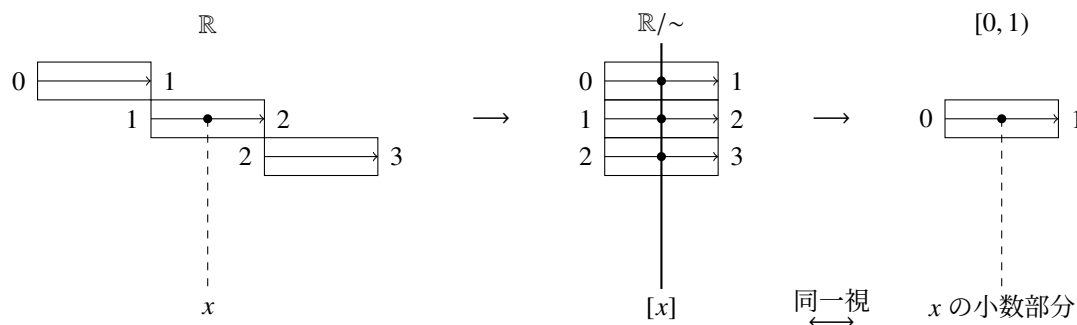
$$x, y \in [\theta] \Rightarrow \sin x = \sin y, \cos x = \cos y.$$

5.5 小数部分

同一視の違う例を見てみよう. 実数の集合 $\mathbb{R}$ 上の二項関係を

$$x \sim y \Leftrightarrow x - y \in \mathbb{Z}$$

で定義する. この関係は同値関係である. このとき, 部分集合 $[0, 1) \subset \mathbb{R}$ は同値関係 $\sim$ の完全代表系である (確かめよ). つまり, 商集合 $\mathbb{R}/\sim$ は $[0, 1)$ と同一視できる. この同一視を図でイメージしてみよう. $\mathbb{R}$ を数直線のテープだと思ふ. 便宜上テープの左端を 0 としておき, 長さ 1 ずつこのテープを切っていく. ただし, 切ったテープの右端はそのテープに含まれないとする. 今, この切ったテープを縦に並べていく. すると, 実数 $x \in \mathbb{R}$ の $\sim$ による同値類 $[x]$ はこの縦長のテープの左端からの距離を表すことになる. 下図の縦の線がこの $[x]$ を表している. 一方, 切ったテープを上重ねていくこと考える. すると (無限の厚みはあるが) 長さ 1 のテープであることには変わらない. これは集合 $[0, 1)$ を表している. したがって, 商集合 $\mathbb{R}/\sim$ は完全代表系 $[0, 1)$ と同一することで, 実数 $x \in \mathbb{R}$ の $\sim$ による同値類 $[x] \in \mathbb{R}/\sim$ は 0 以上 1 未満の実数とみなすことができる. 特にこれは, x の小数部分を表している. 例えば, $[1.3]$ は 0.3, $[\pi]$ は 0.141592... を表していると考えることができる. ただし, 負の数の小数部分は注意が必要 ($[-0.2]$ の小数部分は 0.8 である).



6 順序関係と順序集合

6.1 前順序

$\mathbb{Z}$ 上の関係 $\leq$ (以下) は条件

- (反射律) $\forall x \in X((x, x) \in R) \iff \text{Id}_X \subset R$
- (推移律) $\forall a, b, c \in X((aRb \wedge bRc) \rightarrow aRc) \iff R \circ R \subset R$

の2つの性質を満たしていたことを思い出そう。

定義 6.1. 集合 P 上の関係 $\leq_P$ は反射律と推移律を満たすとき、**前順序** (preorder) であるという。

例 6.2. P をこの講義を受けている学生の集合とする。 P 上の関係として

$$a \leq_P b \iff a \text{ のテストの点数は } b \text{ 以下である}$$

と定義する。任意の $a \in P$ に対し、 a のテストの点数は自身の点数以下であるので、 $a \leq_P a$ 、つまり反射律が成り立つ。また $a \leq_P b$ と $b \leq_P c$ は「 a は b の点数以下」、「 b は c の点数以下」を意味し、「 a は c の点数以下」となるので、これは $a \leq_P c$ を意味する。よって推移律も成り立つ。以上より $\leq_P$ は前順序である。

6.2 反対称的な関係

前順序は $\mathbb{Z}$ 上の「 $\leq$ 」という概念を抽象化しているが、まだ数学的な「順序」としては不十分である。例 6.2 に出てきた $\leq_P$ を考えると、 $a \leq_P b$ かつ $b \leq_P a$ は「 a と b が同じ点数」を意味し、 a と b が同じ人、つまり $a = b$ であるとは限らない。「順序が等しい」と「要素が等しい」が違う意味を持つことになる。一方で $\mathbb{Z}$ 上の「 $\leq$ 」は $a \leq b$ と $b \leq a$ という順序が成り立てば、 a と b は同じ数字、つまり $a = b$ となる。この性質は等号を示すのに非常に重要である。まずはこの性質を「関係」の性質として定義する。

定義 6.3. 集合 X 上の関係 R が**反対称的** (antisymmetric) であるとは、任意の $a, b \in X$ に対して $(a, b) \in R$ かつ $(b, a) \in R$ ならばいつでも $a = b$ であるときにいう。つまり、

$$R \text{ が反対称的である} \iff \forall a, b \in X(aRb \wedge bRa \rightarrow a = b) \iff R \cap R^{-1} \subset \text{Id}_X$$

である。この条件を**反対称律**という。「反対称的」は「対称的ではない」とは違う意味であることに注意する。

例 6.2 の「 $\leq_P$ 」はもし同じ点数を取った人が複数人いれば反対称的ではない。一方で $\mathbb{Z}$ 上の「 $\leq$ 」は反対称的である（むしろ「 $\leq$ 」の性質を抜き出したのだから当たり前である）。もう少し例を見ておこう。

例 6.4. $X = \{1, 2, 3\}$ とし、 X 上の関係を

$$R = \{(1, 1), (1, 2), (1, 3), (3, 2), (3, 3)\}$$

とすると、 R と R^{-1} の有効グラフは次のようになる。



よって $R \cap R^{-1} = \{(1, 1), (3, 3)\} \subset \text{Id}_X$ となり R は反対称的である。関係が反対称的であることと、有効グラフの異なる2頂点には両方向の矢印がないことは同値である。

6.3 半順序

定義 6.5. 集合 P 上の関係 $\leq_P$ は反射律, 推移律, 反対称律を満たすとき, **半順序** (partial order), または単に**順序** (order) という. 半順序の記号としては $\leq_P, \leq_P$ などがよく使われる. また半順序 $\leq_P$ を備えた集合 $(P, \leq_P)$ のことを**半順序集合** (partially ordered set, poset), または単に**順序集合** (ordered set) という. 半順序 $\leq_P$ が文脈から明らかなきときは, $(P, \leq_P)$ を単に P で表すこともある. 半順序集合 $(P, \leq_P)$ と $a, b \in P$ に対し, $a \leq_P b$ かつ $a \neq b$ のときは, $a <_P b$ と書き, $a \leq_P b$ や $a <_P b$ を $b \geq_P a$ や $b >_P a$ と書いたりする. 日本語では $\leq$ と同様に以下, 以上, より小さい, より大きいなどで表現する.

$\mathbb{Z}$ 上の関係 $\leq$ は半順序であり, $(\mathbb{Z}, \leq)$ は半順序集合となる. 一方で, 例 6.2 の $\leq_P$ は反対称的ではないので半順序とはならない. 半順序の具体例を見てみる.

例 6.6. P をこの講義を受けている学生の集合とする. P 上の関係として

$$a \leq_P b \Leftrightarrow a \text{ さんの学籍番号は } b \text{ さんの学籍番号以下である}$$

と定義する. これが反射律と推移律を満たすことは容易に確かめられる. 一方で, 東邦大学内では, 学籍番号は異なる人には異なる番号が与えられているので, $a \leq_P b$ かつ $b \leq_P a$ であれば, $a = b$ である. よって $\leq_P$ は半順序である.

自然数の集合 $\mathbb{N}$ に対し, $(\mathbb{N}, \leq)$ も半順序集合であるが, 同じ集合でも異なる順序を定義することができる. $\mathbb{Z}$ 上の順序で代表的な例を 1 つ見よう.

例 6.7. $\mathbb{N}$ 上の二項関係を

$$a \leq_{\mathbb{N}} b \Leftrightarrow a \text{ は } b \text{ の約数である}$$

で定義する. この関係が半順序となることを見る.

(反射律) 任意の自然数 $x \in \mathbb{N}$ に対し, x は x の約数であるので, $x \leq_{\mathbb{N}} x$ が成り立つ.

(推移律) 任意の自然数 $x, y, z \in \mathbb{N}$ で $x \leq_{\mathbb{N}} y, y \leq_{\mathbb{N}} z$ を満たすものをとる ($x \leq_{\mathbb{N}} y \leq_{\mathbb{N}} z$ とは書かない). このとき, ある自然数 k が存在して, $y = kx$ と書ける. 同様にある自然数 ℓ が存在して $z = \ell y$ と書ける. すると

$$z = \ell y = \ell(kx) = (\ell k)x$$

となり, ℓk は自然数なので, x は z の約数となる. つまり $x \leq_{\mathbb{N}} z$ が成立する (推移律が成り立つことがわかると $x \leq_{\mathbb{N}} y \leq_{\mathbb{N}} z$ と書いてもよい).

(反対称律) 任意の自然数 $x, y \in \mathbb{N}$ で $x \leq_{\mathbb{N}} y, y \leq_{\mathbb{N}} x$ を満たすものをとる. このとき, ある自然数 k と ℓ が存在して, $y = kx, x = \ell y$ と書ける. すると

$$x = \ell y = \ell(kx) = (\ell k)x$$

となり, x が自然数なので, $\ell k = 1$, さらに ℓ, k も自然数なので $\ell = k = 1$ となる. これは $x = y$ を意味する.

以上より, $\leq_{\mathbb{N}}$ は反射律, 推移律, 反対称律を満たすので, $\mathbb{N}$ 上の順序となる.

$\mathbb{N}$ において, 通常の $\leq$ という順序ではどんな自然数にも順序が付いていた. つまり任意の自然数 $x, y \in \mathbb{N}$ に対し, $x \leq y$ または $x \geq y$ が成り立つ. しかし, 例 6.7 の順序 $\leq_{\mathbb{N}}$ では順序が付いていない要素が存在する. 実際, 2 と 3 は互いに約数ではないので, $2 \leq_{\mathbb{N}} 3$ でも $2 \geq_{\mathbb{N}} 3$ でもない.

定義 6.8. $(P, \leq_P)$ を半順序集合とする. $a, b \in P$ に対し, $a \leq_P b$ ではないとき, $a \not\leq_P b$ と書く. $\not\leq_P, \not\leq_P, \not\leq_P$ も同様に定義する. $a \not\leq_P b$ かつ $a \not\geq_P b$ が成り立つとき, a と b は**比較不可能** (incomparable) であるという. 一方, $a \leq_P b$ または $a \geq_P b$ が成り立つときは, a と b は**比較可能** (comparable) であるという. また半順序集合 $(P, \leq_P)$ は任意の $a, b \in P$ に対し, a と b が比較可能であるとき, **全順序集合** (totally ordered set) といい, $\leq_P$ を**全順序** (total order) という.

半順序集合 $(\mathbb{N}, \leq)$ は全順序集合であるが, 例 6.7 の半順序集合 $(\mathbb{N}, \leq_{\mathbb{N}})$ は全順序集合ではない. また「 $\leq$ 」では $\not\leq$ と $>$ は同じ意味であったが, 「 $\leq_{\mathbb{N}}$ 」では $\not\leq_{\mathbb{N}}$ だったとしても, $>_{\mathbb{N}}$ になるとは限らない. 実際, $2 \not\leq_{\mathbb{N}} 3$ であるが, $2 >_{\mathbb{N}} 3$ ではない.

6.4 ハッセ図

半順序は集合上の関係なので、集合が有限であれば、これまで通り有向グラフを使って表すことができる。しかし、そのまま書くと辺の個数が多すぎたりして見にくくなることがある。そこで半順序の3つの条件が成り立つことを意識して、もう少し単純な図として書くことにする。

まず、集合 $P = \{1, 2, 3, 4, 5\}$ 上の関係

$$\leq_P := \{(1, 1), (1, 3), (1, 4), (1, 5), (2, 2), (2, 3), (2, 4), (2, 5), (3, 3), (3, 4), (3, 5), (4, 4), (5, 5)\}$$

を考える。これが半順序となることは各自確かめよう。この半順序は13個の $a \leq_P b$ という情報からできているが、 $\leq_P$ を復元するのに本当にこれだけの情報があるだろうか。例えば、反射律が成り立つため、どんな $i \in P$ に対しても、 $i \leq_P i$ となる。したがって、半順序となることを知っていれば $i \leq_P i$ という情報は書かなくてもわかる。さらに、この半順序では、 $1 \leq_P 3, 1 \leq_P 5, 3 \leq_P 5$ という情報があるが、推移律が成り立つため、 $1 \leq_P 3, 3 \leq_P 5$ がわかっていれば、 $1 \leq_P 5$ が従うので、これもなくてよい。以上のことを考えると、実は $\leq_P$ は

$$1 \leq_P 3, 2 \leq_P 3, 3 \leq_P 4, 3 \leq_P 5$$

という4個の情報さえあれば復元可能である。なお、反対称律から $\leq_P$ ではなく $<_P$ を考えれば十分なものわかるであろう。この必要最低限の情報を定義する。

定義 6.9. $(P, \leq_P)$ を半順序集合とし、 $a <_P b$ となる $a, b \in P$ をとる。もし $a <_P c$ かつ $c <_P b$ となる $c \in P$ が存在しなければ、 $a <_P b$ という関係を被覆関係 (cover relation) といい、 $a <_P b$ と書く。つまり被覆関係とは、中間の要素がない関係のことである。

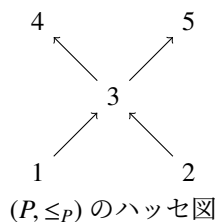
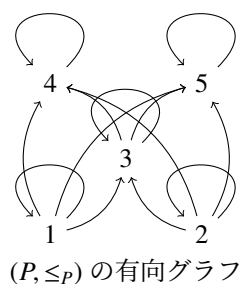
先ほどの例だと、 $\leq_P$ は

$$1 <_P 3, 2 <_P 3, 3 <_P 4, 3 <_P 5$$

という被覆関係全体から復元される。それではこの被覆関係から次の手順で有向グラフを書いてみよう。

1. 頂点を順序が大きいものが上にくるように書く (反対称律から必ずこのように置ける)。
2. 各被覆関係に対して小さいものから大きいものへ矢印を書く。

このようにしてできた有向グラフを $(P, \leq_P)$ のハッセ図 (Hasse diagram) という。先ほどの例で、関係から作る有向グラフとハッセ図の両方を書いてみる。



いかに冗長な情報があったかわかるであろう。またハッセ図を見れば2つの元が比較可能か比較不可能か視覚的にわかる。実際、 $a, b \in P$ が比較可能であることと、 a から b または b から a へ矢印に沿って辿り着けることは同値である。上の図では、1 から $5 \leftarrow 1 \rightarrow 3$ と $3 \rightarrow 5$ の2本の矢印に沿って辿り着けるので、1 と 5 は比較可能である。一方で、1 と 2 は矢印に沿って辿り着けないので、比較不可能である。

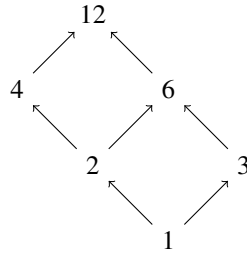
例 6.10. 全順序のハッセ図は非常に単純である。実際、一直線になる。 $P = \{1, 2, 3\}$ とし、通常の意味での「 $\leq$ 」を考えると、 $(P, \leq)$ は全順序である。このハッセ図は以下の通りになる。



例 6.11. n を自然数とし, P を n の約数全体の集合とする. P 上の関係を

$$a \leq_P b \Leftrightarrow a \text{ は } b \text{ の約数である}$$

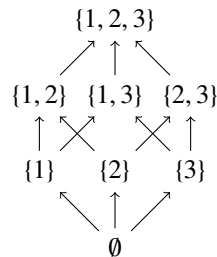
で定義する. 例 6.7 と同様に, この関係も順序関係であることがわかる. $n = 12$ のときに, $(P, \leq_P)$ のハッセ図を書くと次のようになる.



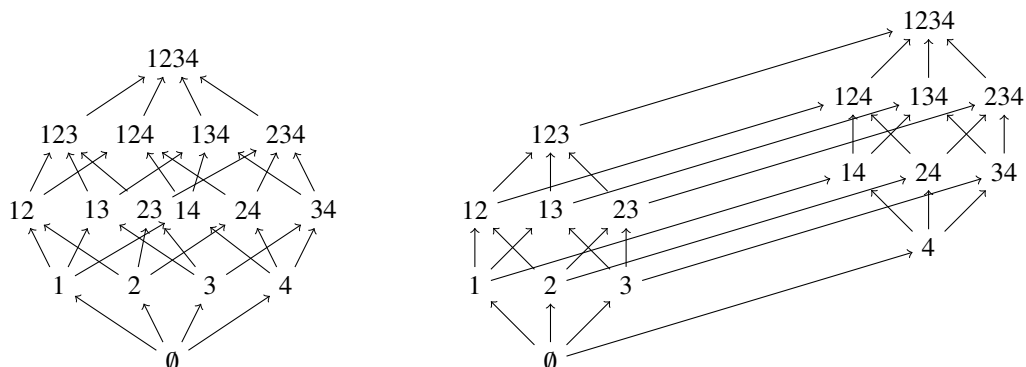
例 6.12. 半順序の代表例を 1 つ紹介する. 集合 $X = \{1, 2, 3\}$ の冪集合 $P = 2^X$ 上の二項関係を

$$A \leq_P B \Leftrightarrow A \subset B$$

で定義する. このとき, $\leq_P$ は半順序である (確かめよ). ここではわざわざ $\leq_P$ で置き直したが, 基本は包含関係による順序として $(P, \leq_P)$ の代わりに $(P, \subset)$ と書く. このときの $(P, \subset)$ のハッセ図は次のとおりである.



このハッセ図をよく見ると立方体の骨組み (辺と頂点) となっていることがわかるであろう. それでは $Y = \{1, 2, 3, 4\}$, $Q = 2^Y$ とし, 包含関係による半順序集合 $(Q, \subset)$ のハッセ図を機械的に書いたものと, 少し場所を意識して書いたものの 2 通り書く.



右の図は, 2 つの立方体 $((P, \subset)$ のハッセ図) を繋いだ形をしている. 立方体は 2 つの正方形を繋いだ形であった. 実は, $(Q, \subset)$ のハッセ図は 4 次元の立方体 (4 次元超立方体) の骨組みとなっている. より一般に $[n] := \{1, 2, \dots, n\}$, $P_n = 2^{[n]}$ とすると, 半順序 $(P_n, \subset)$ のハッセ図は n 次元超立方体 (hypercube) の骨組みとなる.

7 最大・最小/極大・極小/上界・下界/上限・下限

7.1 極大・極小/最大・最小

これまで、最大や最小という言葉は自然と用いてきた。その用語を順序集合において厳密に定義する。

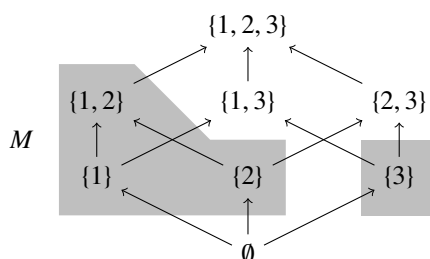
定義 7.1. $(P, \leq_P)$ を順序集合, M を P の空でない部分集合とする。このとき,

- $a <_P x$ となる $x \in M$ が存在しない M の元 a を M の**極大元** (maximal element) という。
- $x <_P b$ となる $x \in M$ が存在しない M の元 b を M の**極小元** (minimal element) という。

例 7.2. $X = \{1, 2, 3\}, P = 2^X$ とし包含関係による順序集合 $(P, \subset)$, さらに P の部分集合として

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

を考える。このとき, M の極大元は $\{1, 2\}$ と $\{3\}$ であり, 極小元は $\{1\}, \{2\}, \{3\}$ である。



このように,

- 極大 (小) 元は複数存在することがある
- 極大かつ極小となる元が存在することがある

ということがわかる。さらに次が成り立つ。

命題 7.3. $(P, \leq_P)$ を順序集合, M を P の空でない部分集合とする。 $a, b \in M$ が M の異なる極大 (小) 元の時, a と b は比較不可能である。

Proof. 背理法で証明する。極大元 a と b が比較可能であったとすると, $a \leq_P b$ または $a \geq_P b$ が成り立つ。 $a \leq_P b$ としてよい。特に, $a \neq b$ であるので, $a <_P b$ である。しかし, a は M の極大元なので, $a <_P x$ となる x は M に存在しない。よって矛盾が起こるので, a と b は比較不可能である。

極小元の場合も同様に証明できる。 □

上の例では極大元, 極小元の両方が存在していたが, 存在しない場合もある。存在しない例はあとで見るが, ここでは有限集合であればいつでも極大 (小) 元を持つことを見る。

命題 7.4. $(P, \leq_P)$ を順序集合とし, M を P の空でない有限部分集合とする。このとき, P は極大 (小) 元を少なくとも 1 個持つ。

Proof. M の元の個数を n とし, n に関する帰納法で証明する。 $n = 1$ のときは, $M = \{a\}$ とすると, $a <_P x$ となる M の元 x が存在しないので, a は極大元である。 $n \geq 2$ とする。 M の元 a を 1 つ選び, $N = M \setminus \{a\}$ とすると, N の元の個数は $n - 1$ である。よって, 帰納法の仮定から N は極大元を持つ。それを b とする。 b が M の極大元であれば, 証明は完結する。 b が M の極大元でなければ, $b <_P x$ となる, $x \in M$ が存在する。 b は N の極大元であるので, $x \notin N$ である。つまり, $x = a$ である。特に, a は M の極大元となっている。実際, a が M の極大元でなければ, $a <_P y$ となる $y \in M$ が存在するが, これは $y \in N$ であり, $b <_P a <_P y$ となるので, b が N の極大元であることに矛盾する。以上より, M は極大元を持つ。

極小元の場合も同様に証明できる。 □

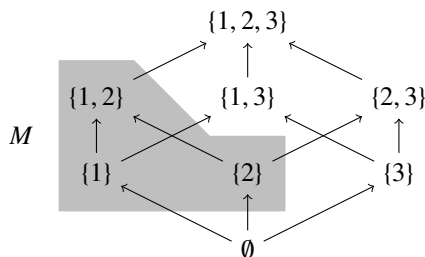
定義 7.5. $(P, \leq_P)$ を順序集合, M を P の空でない部分集合とする. このとき,

- 任意の $x \in M$ に対して, $x \leq_P a$ となる M の元 a を, M の**最大元** (maximum element) といい, $\max(M)$ で表す.
- 任意の $x \in M$ に対して, $b \leq_P x$ となる M の元 b を, M の**最小元** (minimum element) といい, $\min(M)$ で表す.

例 7.6. $X = \{1, 2, 3\}, P = 2^X$ とし包含関係による順序集合 $(P, \subset)$, さらに P の部分集合として

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

を考える. このとき, M の最大元は $\{1, 2\}$ であり, 最小元は存在しない.



このように,

- (有限集合であったとしても) 最大 (小) 元は存在するとは限らない

ことがわかる. さらに次が成り立つ.

命題 7.7. 順序集合 $(P, \leq_P)$ に対して, 空でない P の部分集合 M の最大 (小) 元は, 存在すれば唯一である. また最大 (小) は極大 (小) 元である.

Proof. M の最大元が 2 個存在すると仮定する. そこで, $a_1, a_2 \in M$ (ただし $a_1 \neq a_2$) を M の最大元とする. a_1 は最大元なので, 任意の $x \in M$ に対して, $x \leq_P a_1$, 特に $a_2 \leq_P a_1$ である. 同様に, a_2 も最大元なので, 任意の $x \in M$ に対して, $x \leq_P a_2$, 特に $a_1 \leq_P a_2$ である. ところが, $\leq_P$ は順序関係であるので, 反対称律が成り立つ. これは $a_1 = a_2$ を意味し, 矛盾. よって M の最大元は, 存在すれば唯一である. また, a を M の最大元であるとする. a が M の極大元でないと仮定すると, $a <_P x$ となる $x \in M$ が存在する. しかし, a は M の最大元であるので, 任意の $y \in M$ に対し, $y \leq_P a$ が成り立つ. 特に $x \leq_P a$ である. よって $x \leq_P a <_P x$ となり, 矛盾する. 以上より, a は極大元である.

最小元の場合も同様に証明できる. □

7.2 上界・下界/上限・下限

定義 7.8. $(P, \leq_P)$ を順序集合, M を P の空でない部分集合とする. このとき,

- 任意の $x \in M$ に対して, $x \leq_P a$ となる P の元 a を, M の P における**上界** (upper bound) という. M の上界の全体を $U(M)$, つまり

$$U(M) = \{a \in P : \text{すべての } x \in M \text{ に対し } x \leq_P a\}$$

とする. また, 任意の $x \in M$ に対して, $b \leq_P x$ となる P の元 b を, M の P における**下界** (lower bound) という. M の下界の全体を $L(M)$, つまり

$$L(M) = \{b \in P : \text{すべての } x \in M \text{ に対し } b \leq_P x\}$$

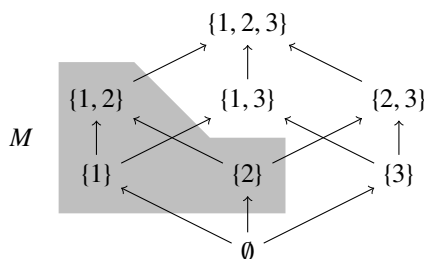
とする.

- M が P において上界をもつ、つまり $U(M) \neq \emptyset$ のときは、**上に有界**といい、下界をもつ、つまり $L(M) \neq \emptyset$ のときは、**下に有界**という。さらに M が上界も下界ももつときは、**有界**という。
- $U(M) \neq \emptyset$ かつ $\min(U(M))$ が存在するとき、これを**最小上界** (least upper bound), または**上限** (supremum) といい、 $\sup(M)$ で表す。また、 $L(M) \neq \emptyset$ かつ $\max(L(M))$ が存在するとき、これを**最大下界** (greatest lower bound), または**下限** (infimum) といい、 $\inf(M)$ で表す。

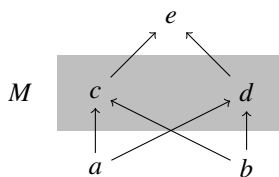
例 7.9. $X = \{1, 2, 3\}, P = 2^X$ とし包含関係による順序集合 $(P, \subset)$, さらに P の部分集合として

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

を考える。このとき、 M の上界は $\{1, 2\}$ と $\{1, 2, 3\}$ であり、上限は $\{1, 2\}$ である。一方、 M の下界は $\emptyset$ であり、これは下限でもある。



例 7.10. $P = \{a, b, c, d, e\}$ に対し、順序集合 $(P, \leq_P)$ を次のハッセ図で定義する。



$M = \{c, d\}$ とすると、 M の上界は e であり、上限は e である。一方、 M の下界は a と b であり、下限は存在しない。

このように、

- 上界や下界が存在しても、上限や下限が存在するとは限らない
- 上限や下限は M の中にあるとは限らない

ということがわかる。さらに、次の命題が成り立つ。

命題 7.11. $(P, \leq_P)$ を順序集合、 M を P の空でない部分集合とする。このとき、

$$1. \sup(M) \in M \Rightarrow \sup(M) = \max(M),$$

$$2. \inf(M) \in M \Rightarrow \inf(M) = \min(M).$$

Proof. (1) $a = \sup(M)$ とする。このとき定義から、任意の $x \in M$ に対し、 $x \leq_P a$ が成り立つ。 $a \in M$ であるので、これは a が M の最大元であるという定義を満たす。

(2) (1) と同様。 □

これまでの例は全て有限集合であったが、無限集合で考えると、異なる状況が生じる。例えば、極大 (小) 元は無限集合の場合存在するとは限らない。

例 7.12. $\mathbb{R}$ を実数全体の集合とし、通常不等号 $\leq$ を用いた順序集合 $(\mathbb{R}, \leq)$ を考える。さらに、 $\mathbb{R}$ の部分集合として

$$M = \{x \in \mathbb{R} : 0 \leq x < \sqrt{2}\}$$

とする。このとき、 M の最大元、最小元、上限、下限を求める。

数直線で考えると、 M の上界全体の集合は $U(M) = \{x \in \mathbb{R} : \sqrt{2} \leq x\}$ である。特に、 M の上限は $\sup(M) = \sqrt{2}$ である。このとき、 M の上限は M に属さない、つまり $\sup(M) \notin M$ である。一方、 M の下界全体の集合は $L(M) = \{x \in \mathbb{R} : x \leq 0\}$ である。特に、 M の下限は $\inf(M) = 0$ であり、 $\inf(M) \in M$ となっている。よって命題 7.11 より M の最小元は $\min(M) = \inf(M) = 0$ である。

M は極大元を持たない、特に最大元を持たないことを示す。 M が極大元 a を持ったとする。このとき、 $a < \sqrt{2}$ である。 $0 < \sqrt{2} - a$ であるので、

$$a < a + \frac{(\sqrt{2} - a)}{2} < a + (\sqrt{2} - a) = \sqrt{2}$$

が成り立つ。よって $b = a + \frac{(\sqrt{2} - a)}{2}$ とすると、 $b \in M$ となることがわかる。しかし、これは a が M の極大元であることに矛盾する。よって M は極大元を持たない。

例 7.13. $\mathbb{R}$ を有理数全体の集合とし、通常不等号 $\leq$ を用いた順序集合 $(\mathbb{R}, \leq)$ を考える。さらに、 $\mathbb{R}$ の部分集合として

$$M = \left\{ \frac{1}{n} : n \in \mathbb{N} \right\}$$

とする。ここで、 $\mathbb{N}$ は自然数全体の集合である。このとき、 M の最大元、最小元、上限、下限を求める。

任意の自然数 $n \in \mathbb{N}$ に対し、

$$0 < \frac{1}{n} \leq \frac{1}{1} = 1$$

なので、 M の上界全体の集合は $U(M) = \{x \in \mathbb{R} : 1 \leq x\}$ である。特に、 M の上限は $\sup(M) = 1$ である。このとき、 $\sup(M) \in M$ であるので、命題 7.11 より M の最大元は $\max(M) = \sup(M) = 1$ である。

一方、 M の下界全体の集合は $L(M) = \{x \in \mathbb{R} : x \leq 0\}$ である。特に、 M の下限は $\inf(M) = 0$ である。このとき、 $\inf(M) \notin M$ となっていることに注意する。

M は極小元をもたない、特に最小元を持たないことを示す。 M が極小元 a を持ったとする。 $a \in M$ であるので、ある自然数 $n \in \mathbb{N}$ を使って、 $a = \frac{1}{n}$ と書ける。このとき、

$$\frac{1}{n+1} < \frac{1}{n} = a$$

が成り立ち、 $\frac{1}{n+1} \in M$ であるので、これは a が M の極小元であることに矛盾する。よって M は極小元を持たない。

注意 7.14. 極大（小）元は「境界（端）の点」というイメージであり、上記 2 つの例の極大（小）元を持たない証明は、点を適当にとったとき、それより遠い点が範囲内でとれ、さらにそれより遠い点が範囲内でとれ、…とこの操作が延々と繰り返されていつまで経っても境界（端）に辿りつかない、つまり境界（端）が存在しないということで証明している。

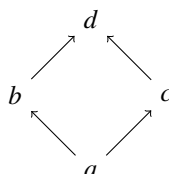
8 束

8.1 束

上限と下限は有限集合であったとしても、いつも存在するとは限らないことを見た。この節では、有限部分集合がいつでも上限と下限を持つような順序集合に着目して、その性質を調べる。

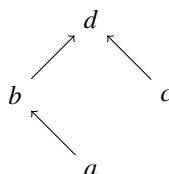
定義 8.1. 順序集合 $(L, \leq_L)$ が束 (lattice) であるとは、 L の任意の空でない有限部分集合に対して、上限と下限が存在するときをいう。

例 8.2. $L = \{a, b, c, d\}$ に対し、順序集合 $(L, \leq_L)$ を次のハッセ図で定義する。



このとき、 L の 1 元からなる集合は自身を上限、下限に持ち、2 元からなる集合、例えば、 $\{a, b\}$ なら、上限 b 、下限 a を持ち、 $\{b, c\}$ なら上限 d 、下限 a を持つ。この議論を続けると、すべての空でない有限部分集合は上限と下限を持つことがわかるので、 $(L, \leq_L)$ は束である。

例 8.3. $L = \{a, b, c, d\}$ に対し、順序集合 $(L, \leq_L)$ を次のハッセ図で定義する。



このとき、 L 全体では上限 d を持つが、下限は持たない。特に、2 元からなる集合 $\{a, c\}$ も下限を持たない。よって $(L, \leq_L)$ は束ではない。

順序集合が束であるためには、すべての空でない有限部分集合に対して、上限と下限の存在を確認しないといけないが、実は、2 元からなる集合だけ確認すれば十分である。

定理 8.4. 順序集合 $(L, \leq_L)$ が束となる必要十分条件は、 L の任意の 2 元 $x, y \in L$ に対し、 $\{x, y\}$ が上限と下限を持つことである。

Proof. $\Rightarrow$ は束の定義から明らか。 $\Leftarrow$ を示す。これは、任意の 2 元 $x, y \in L$ に対し、 $\{x, y\}$ が上限と下限を持てば、 L の任意の空でない有限部分集合は上限と下限を持つことを示せばよい。

L の任意の空でない有限部分集合 M をとり、 M の元の個数 n に関する帰納法で証明する。 $n = 1$ のとき、 $M = \{a_1\}$ とすると、 a_1 は M の上限かつ下限である。 $n \geq 2$ と仮定し、 $M = \{a_1, \dots, a_n\}$ とする。帰納法の仮定から $N = M \setminus \{a_n\} = \{a_1, \dots, a_{n-1}\}$ は上限と下限を持つ。その上限を $\sup(N) = a$ とする。このとき、 $a_1, \dots, a_{n-1} \leq a$ である。仮定から、 $\{a, a_n\}$ は上限を持つので、それを a' とする。すると、 $a, a_n \leq a'$ が成り立つ。特に、

$$a_1, \dots, a_n \leq a'$$

である。よって a' は M の上界である。

a' が M の上限であることを示す。 M の任意の上界 u をとる。このとき、 $a_n \leq u$ が成り立つ。また a は N の上限、つまり最小上界であり、 u は N の上界でもあるので、 $a \leq u$ である。よって u は $\{a, a_n\}$ の上界である。 a' は $\{a, a_n\}$ の上限であったので、 $a' \leq u$ が成り立つ。よって a' が M の最小上界であることがわかるので、 a' は M の上限である。

M が下限を持つことも同様に証明できる。

□

8.2 結びと交わり

上限と下限はそれぞれ上界と下界の最大元と最小元であった。最大元と最小元は存在すれば唯一であったことを思い出そう。よって、もし $(L, \leq_P)$ が束であれば、 L の任意の 2 元 $x, y \in L$ に対し、 $\{x, y\}$ の上限、下限がただ 1 つ決まる。それを $x \vee y$ と $x \wedge y$ で表し、 x と y の**結び** (join) と**交わり** (meet) と呼ぶ。つまり、

$$x \vee y := \sup(\{x, y\}), \quad x \wedge y := \inf(\{x, y\})$$

である。

x と y が比較可能であれば $\vee$ と $\wedge$ を計算することは容易である。

命題 8.5. $(L, \leq_L)$ を束とし、 $x, y \in L$ とする。このとき、次の 3 条件は同値である。

1. $x \leq_L y$,
2. $x \vee y = y$,
3. $x \wedge y = x$,

Proof. (1) $\Rightarrow$ (2) を示す。(1) より y は $\{x, y\}$ の上界である。かつてな $\{x, y\}$ の上界 u をとると、 $y \leq_P u$ が成り立つので、 y は最小上界、つまり $\{x, y\}$ の上限である。よって $x \vee y = y$ である。

次に (2) $\Rightarrow$ (1) を示す。(2) より y は $\{x, y\}$ の上限である。このとき、 $y = \sup(\{x, y\}) \in \{x, y\}$ であるので、前回の命題 8.11 より y は $\{x, y\}$ の最大元である。よって $x \leq_P y$ が成り立つ。

(1) $\Leftrightarrow$ (3) は同様に証明できる。 □

この $\vee$ や $\wedge$ は束 $(L, \leq_L)$ における和と積だと考える。この演算に対し、以下の性質が成り立つ（証明は省略）。

定理 8.6. $(L, \leq_P)$ を束とし、 $x, y, z \in L$ とする。このとき、次が成り立つ。

$$\begin{array}{ll} \text{(交換律)} & x \vee y = y \vee x \qquad x \wedge y = y \wedge x \\ \text{(結合律)} & (x \vee y) \vee z = x \vee (y \vee z) \quad (x \wedge y) \wedge z = x \wedge (y \wedge z) \\ \text{(冪等律)} & x \vee x = x \qquad x \wedge x = x \\ \text{(吸収律)} & x \wedge (x \vee y) = x \qquad x \vee (x \wedge y) = x \end{array}$$

さらに、 L が有限集合のとき、 L の最大元 $\top$ と最小元 $\perp$ が存在し、次が成り立つ。

$$\begin{array}{ll} \text{(最大元の性質)} & \top \wedge x = x \quad \top \vee x = \top \\ \text{(最小元の性質)} & \perp \wedge x = \perp \quad \perp \vee x = x \end{array}$$

この性質を用いることで、上限や下限について計算ができる。例えば、

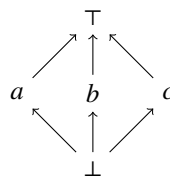
$$(x \wedge \perp) \vee (\top \wedge y) \stackrel{\text{交換律}}{=} (\perp \wedge x) \vee (\top \wedge y) \stackrel{\text{最小元の性質}}{=} \perp \vee (\top \wedge y) \stackrel{\text{最小元の性質}}{=} \top \wedge y \stackrel{\text{最大元の性質}}{=} y$$

のように計算できる。しかし、束の和と積の演算では、分配法則が成り立つとは限らない。ここで分配法則（分配律）とは、

$$\begin{array}{ll} \text{(分配律 1)} & x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z) \\ \text{(分配律 2)} & x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z) \end{array}$$

という性質である。

例 8.7. $L = \{a, b, c, \top, \perp\}$ に対し、順序集合 $(L, \leq_L)$ を次のハッセ図で定義する。



L が束となることの確認は各自にまかせる．このとき，

$$a \vee b = b \vee c = a \vee c = \top$$

$$a \wedge b = b \wedge c = a \wedge c = \perp$$

であるので，

$$a \vee (b \wedge c) = a \vee \perp = a \neq \top = \top \wedge \top = (a \vee b) \wedge (a \vee c)$$

であり，分配律が成り立たない $a, b, c \in L$ が存在する．

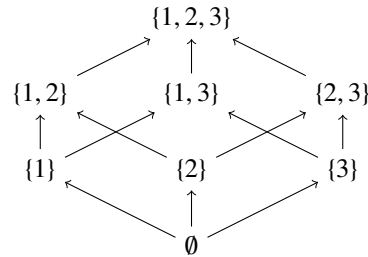
8.3 分配束とモジュラー束

定義 8.8. 束 $(L, \leq_L)$ は，任意の $x, y, z \in L$ に対し，分配律が成り立つとき，**分配束** (distributive lattice) と呼ばれる．

例 8.9. $X = \{1, 2, 3\}, L = 2^X$ とし包含関係による順序集合 $(L, \subset)$ を考える．このとき， $(L, \subset)$ は束である．注意深く考えると，この束の和と積は，集合の和集合と積集合である．つまり， $A, B \in L$ に対し，

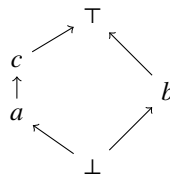
$$A \vee B = A \cup B, \quad A \wedge B = A \cap B$$

である（これが記号として $\vee$ と $\wedge$ を使う理由でもある）．集合の和と積は分配法則が成り立っていたことを思い出すと， $(L, \subset)$ が分配束となることがわかる．



分配束は，集合の和集合や積集合の計算とほぼ同じ感覚で上限や下限の計算を行うことができる．次に，もう 1 つ分配束とならない例を見てみよう．

例 8.10. $L = \{a, b, c, \top, \perp\}$ に対し，順序集合 $(L, \leq_L)$ を次のハッセ図で定義する．



L が束となることの確認は各自にまかせる．このとき，

$$a \vee b = b \vee c = \top$$

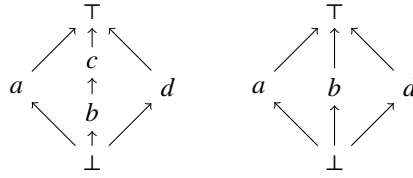
$$a \wedge b = b \wedge c = \perp$$

であり， $a \vee c = c$ かつ $a \wedge c = a$ なので，

$$a \vee (b \wedge c) = a \vee \perp = a \neq c = \top \wedge c = (a \vee b) \wedge (a \vee c)$$

であり，分配律が成り立たない $a, b, c \in L$ が存在する．よって $(L, \leq_P)$ は分配束ではない．

実は、例 8.7 と 8.10 は分配束ではない本質的な束である．束 $(L, \leq_L)$ と L の部分集合 M に対し、任意の $a, b \in M$ が $a \vee b, a \wedge b \in M$ を満たしているとき、 $(M, \leq_L)$ を $(L, \leq_L)$ の部分束 (sublattice) という．例えば、下の束 $\{\top, a, b, c, d, \perp\}$ に対し、部分集合 $\{\top, a, b, d, \perp\}$ は部分束である．



証明はしないが分配束は次のように特徴づけることができる．

定理 8.11 (Birkhoff). 束 $(L, \leq_L)$ が分配束となる必要十分条件は、 $(L, \leq_L)$ が



というハッセ図で表される部分束を持たないことである．

この結果により、分配束かどうかはハッセ図を書けば視覚的にある程度わかる．例えば、定理の直前の束とその部分束はともに分配束ではない．

さて、数の通常の演算において和と積の順番を入れ替えることはできない．例えば、 $(1+2) \times 2 \neq 1 + (2 \times 2)$ である．しかし、分配束 $(L, \leq_L)$ は次のような性質を持つ． $x, y, z \in L$ に対し、

$$(\text{モジュラー律}) \quad x \leq_L y \Rightarrow (x \vee z) \wedge y = x \vee (z \wedge y).$$

定義 8.12. 束 $(L, \leq_L)$ は、任意の $x, y, z \in L$ に対し、モジュラー律が成り立つとき、**モジュラー束** (modular lattice) と呼ばれる．

定理 8.13. 分配束はモジュラー束である．

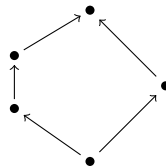
Proof. $(L, \leq_L)$ をかつてな分配束とし、任意の $x, y, z \in L$ で、 $x \leq_L y$ となるものをとる．このとき、

$$(x \vee z) \wedge y \stackrel{\text{分配律}}{=} (x \wedge y) \vee (z \wedge y) \stackrel{\text{命題 8.5}}{=} x \vee (z \wedge y).$$

よってモジュラー律が成り立つので、 $(L, \leq_L)$ はモジュラー束である． □

この定理の逆は成り立たない．実際、定理 8.11 と同じように、モジュラー束も特徴づけが知られており、それらを比べると例 8.7 はモジュラー束であるが、分配束ではないことがわかる．

定理 8.14 (Dedekind). 束 $(L, \leq_L)$ がモジュラー束となる必要十分条件は、 $(L, \leq_L)$ が



というハッセ図で表される部分束を持たないことである．

例 8.10 がモジュラー束とならないことは、 $a \leq_L c$ であるが、

$$(a \vee b) \wedge c = \top \wedge c = c \neq a = a \vee \perp = a \vee (b \wedge c)$$

よりわかる．

束には他にも様々な興味深い性質がある、束を中心的に取り扱う理論を**束理論**と呼ぶ．

9 自然数

9.1 自然数の定義

子どもの頃から「数」というものを使ってきたと思うが、そもそも「数」の定義は言えるだろうか。実は、高校まで「数」というものは定義されずに使われている。「数」というものはなんとなくわかるし、その理解で十分であった。しかし、数学の本質の1つは概念や事象を（数学的に）言語化することである。今回は、自然数を厳密に定義する。普段、0は自然数に入れない派だが、あとの話題のために0は自然数として定義していく。

定義 9.1 (ペアノの公理系). 自然数は以下の条件を満たすものである。

(P1) 0は自然数である（ここで0は単なる記号）。

(P2) n が自然数ならば、その後者（successor）となる自然数がただ1つ存在する（これを S_n と書く）。

(P3) $S_n = 0$ となる自然数 n は存在しない（つまり、0の前者となる自然数は存在しない）。

(P4) 異なる2つの自然数 n と m の後者は異なる（つまり、 $S_n \neq S_m$ ）。

(P5) 集合 X について、 $0 \in X$ であり、 X に含まれる任意の自然数 n について $S_n \in X$ となるとき、 X はすべての自然数を含む。

数学は、ある仮定の下、命題を示し、その命題が成り立つと仮定して、新しい命題を示すという流れを辿るが、この流れを逆に辿っていくと、ある時点で証明ができない仮定が現れる。このような仮定は証明なしで成り立つことを認める必要があり、その仮定（前提条件）を**公理** (axiom) といい、公理の集まりを公理系という。上の条件 (P1) から (P5) が普段使っている自然数で成り立つことはわかるであろう。この条件を自然数が満たす公理（前提条件）として、それを自然数の定義としている。

上の公理系より次のことが順番に言える：

(P1) より 0 は自然数なので、(P2) より S_0 も自然数である（これを 1 という記号で書く）。

1 は自然数なので、(P2) より S_1 も自然数である（これを 2 という記号で書く）。

...

こうして、これまで使ってきた $1, 2, 3, \dots$ は $S_0, S_1, S_2, \dots$ を表す記号として導くことができる。以下、自然数全体の集合を $\mathbb{N}$ とする。

公理 (P5) は**数学的帰納法の原理**と呼ばれる。そもそも**数学的帰納法**とは、自然数 n に関する性質 $P(n)$ が以下を満たせば、自然数全体で成立することをいう：

1. $P(0)$ は正しい。
2. 任意の自然数 k で $P(k)$ が正しいならば $P(S_k)$ も正しい。

$P(k)$ が成立している自然数 k の全体の集合を X とすれば、(1), (2) は (P5) の仮定を満たしているので、 $\mathbb{N} \subset X$ が成り立ち、 $X = \mathbb{N}$ となる。よって数学的帰納法が正しいことを保証している。この (P5) を使って、自然数についての様々な性質を導くことができる。

定理 9.2. すべての自然数は $SS \cdots S0$ という形（ S が 0 個以上並んでいる）をしている。

Proof. $X = \{x : x \text{ は } SS \cdots S0 \text{ という形}\}$ とすると、 S が 0 個並んだものは 0 であるので、 $0 \in X$ である。また $n \in X$ とすると、

$$S_n = S \left(\underbrace{SS \cdots S0}_{=n} \right)$$

より $S_n \in X$ である。よって (P5) より $\mathbb{N} \subset X$ 、つまり $\mathbb{N} = X$ である。 □

この主張より、自然数といえるのは $0, 1, 2, \dots$ のようなものだけであることがいえる。また (P1) は 0 という記号から始めたが、別に記号はなんでもいいので、1 に変えても良い。つまり、自然数に 0 を入れるかどうかはペアノの公理系としてはどちらでもいいのである。

9.2 自然数の加法

自然数 $n \in \mathbb{N}$ を固定し、関数 $f_n : \mathbb{N} \rightarrow \mathbb{N}$ を

$$f_n(0) = n, \quad f_n(Sm) = Sf_n(m)$$

で定義する。例えば、 $f_n(3)$ は

$$f_n(3) = f_n(SSS0) = Sf_n(SS0) = SSf_n(S0) = SSSf_n(0) = SSSn$$

となる。つまり $f_n(3)$ は n の 3 個後の自然数を表す。一般に、 $f_n(m)$ は n の m 個後の自然数を表す。ここで、 $f_n(m)$ を $n + m$ で書くこととする。これが自然数における加法の定義である。

この定義を使うと、 $1 + 1 = 2$ であることは、

$$1 + 1 = f_1(1) = f_1(S0) = Sf_1(0) = S1 = 2$$

からわかる。さらに $2 + 3 = 5$ であることは、

$$2 + 3 = f_2(3) = f_2(S2) = f_2(SS1) = f_2(SSS0) = Sf_2(SS0) = SSf_2(S0) = SSSf_2(0) = SSS2 = SS3 = S4 = 5$$

で計算できる。

それでは、この定義に則り、自然数の加法が満たす性質を証明していく。

定理 9.3 (自然数の加法の性質). 自然数 $n, m, k \in \mathbb{N}$ に対し、次の性質が成り立つ。

1. $n + 0 = n$ (0 は加法の**単位元**と呼ばれる)。
2. $n + 1 = Sn$.
3. $n + Sm = Sn + m = S(n + m)$.
4. $n + (m + k) = (n + m) + k$ (加法の結合律)。
5. $n + m = m + n$ (加法の交換律)。

Proof. (1) $n + 0 = f_n(0) = n$.

(2) $n + 1 = f_n(1) = f_n(S0) = Sf_n(0) = Sn$.

(3) 一つ目の等号を証明する。まず $m = 0$ のときを示す。 $n + S0 = n + 1 \stackrel{(2)}{=} Sn \stackrel{(1)}{=} Sn + 0$ より正しい。次に、 $n + Sm = Sn + m$ (★) が成り立つと仮定する。これは $f_n(Sm) = f_{Sn}(m)$ を意味する。このとき、

$$n + SSm = f_n(SSm) = Sf_n(Sm) \stackrel{(\star)}{=} Sf_{Sn}(m) = f_{Sn}(Sm) = Sn + Sm$$

となるので、数学的帰納法より 1 つ目の等号は成り立つ。

また $n + Sm = f_n(Sm) = Sf_n(m) = S(n + m)$ より 2 つ目の等号も正しい。

(4) まず $k = 0$ のときを示す。

$$n + (m + 0) \stackrel{(1)}{=} n + m \stackrel{(1)}{=} (n + m) + 0.$$

次に $n + (m + k) = (n + m) + k$ (★★) が成り立つと仮定すると、

$$n + (m + Sk) \stackrel{(3)}{=} n + S(m + k) = S(n + (m + k)) \stackrel{(\star\star)}{=} S((n + m) + k) \stackrel{(3)}{=} (n + m) + Sk$$

となるので数学的帰納法から加法の結合律は成り立つ。

(5) まず $m = 0$ のときを n に関する帰納法で示す. $n = 0$ のとき, $0 + 0 = 0 + 0$ であるので成り立つ. $n + 0 = 0 + n$ (♯) が成り立つと仮定する. これは $f_n(0) = f_0(n)$ を意味する. このとき, $S_n + 0 \stackrel{(3)}{=} S(n + 0) = S_f(0) \stackrel{(♯)}{=} S_f(n) = f_0(Sn) = 0 + Sn$ となるので数学的帰納法から $m = 0$ のときの加法の交換律が成り立つ.

次に一般の場合を m に関する帰納法で示す. $m = 0$ は今示したことであるので, $n + m = m + n$ (♯♯) を仮定する. このとき,

$$n + Sm \stackrel{(3)}{=} S(n + m) \stackrel{(♯♯)}{=} S(m + n) \stackrel{(3)}{=} Sm + n$$

となるので数学的帰納法から加法の交換法則は成り立つ. □

定理 9.3 の (1) の性質がある意味 0 というものを定義している. 実際, 0 以外で (1) の性質, つまりどんな自然数 $n \in \mathbb{N}$ に対しても $n + a = n$ となるような自然数 a は存在しない. この 0 のように, どんな元に対しても, その加法の結果が変わらない元のことを**加法の単位元**という. 一般に加法の単位元は存在すれば一意である.

定理 9.4 (加法の単位元の一意性). 自然数 $a \in \mathbb{N}$ が任意の自然数 $n \in \mathbb{N}$ に対して $n + a = n$ を満たせば $a = 0$ である.

Proof. n として 0 をとれば $0 + a = 0$ が成り立つ. 一方, 定理 9.3 の (1) より $a + 0 = a$ である. さらに加法の交換律より $a = a + 0 = 0 + a = 0$ が従う. □

9.3 自然数の乗法

自然数 $n \in \mathbb{N}$ を固定し, 関数 $g_n : \mathbb{N} \rightarrow \mathbb{N}$ を

$$g_n(0) = 0, \quad g_n(Sm) = n + g_n(m)$$

で定義する. 例えば, $g_n(3)$ は

$$g_n(3) = g_n(SSS0) = n + g_n(SSn) = n + (n + g_n(S0)) = n + (n + (n + g_n(0))) = n + (n + (n + 0)) = n + (n + n)$$

となる. つまり, $g_n(3)$ は $n + n + n$ (n の 3 倍の自然数) を表す. 一般に, $g_n(m)$ は n の m 倍の自然数を表す. ここで, $g_n(m)$ を $n \cdot m$ で書くこととする. これが自然数における乗法の定義である. この定義を使うと $3 \cdot 2 = 6$ であることは,

$$3 \cdot 2 = g_3(2) = g_3(SS0) = 3 + (g_3(S0)) = 3 + (3 + g_3(0)) = 3 + (3 + 0) = 6$$

で計算できる.

定理 9.5 (自然数の乗法の性質). 自然数 $n, m, \ell \in \mathbb{N}$ に対し, 次の性質が成り立つ.

1. $n \cdot 0 = 0 \cdot n = 0$.
2. $n \cdot 1 = 1 \cdot n = n$ (1 は乗法の**単位元**と呼ばれる).
3. $n \cdot m = m \cdot n$ (乗法の交換律).
4. $n \cdot (m \cdot \ell) = (n \cdot m) \cdot \ell$ (乗法の結合律).
5. $n \cdot (m + \ell) = (n \cdot m) + (n \cdot \ell)$ (分配律)

Proof. (1) まず $n \cdot 0 = g_n(0) = 0$ である. $0 \cdot n = 0$ を帰納法で示す. $n = 0$ の場合はすでに示したので, $0 \cdot n = 0$ が成り立つと仮定する. すると, $0 \cdot Sn = g_0(Sn) = 0 + g_0(n) = g_0(n) = 0 \cdot n = 0$ となり数学的帰納法から (1) が成り立つ.

(2) まず $n \cdot 1 = g_n(1) = g_n(S0) = n + g_n(0) = n + 0 = n$ である. $1 \cdot n = n$ を帰納法で示す. $n = 0$ のときは, (1) から従う. $1 \cdot n = n$ を仮定する. すると, $1 \cdot Sn = g_1(Sn) = 1 + g_1(n) = 1 + 1 \cdot n = 1 + n = Sn$ となり数学的帰納法から (2) が成り立つ.

最後に, (3) と (4) は省略し, (5) を証明する. ℓ に関する帰納法で示す. $\ell = 0$ のとき,

$$n \cdot (m + 0) = n \cdot m = n \cdot m + 0 \stackrel{(1)}{=} (n \cdot m) + (n \cdot 0)$$

から従う. $n \cdot (m + \ell) = (n \cdot m) + (n \cdot \ell)$ (h) が成り立つと仮定する. すると

$$\begin{aligned} n \cdot (m + S\ell) &= n \cdot S(m + \ell) = g_n(S(m + \ell)) = n + g_n(m + \ell) = n + n \cdot (m + \ell) \stackrel{(h)}{=} n + ((n \cdot m) + (n \cdot \ell)) \\ &= (n \cdot m) + (n + n \cdot \ell) = (n \cdot m) + (n + g_n(\ell)) = (n \cdot m) + (g_n(S\ell)) = (n \cdot m) + (n \cdot S\ell) \end{aligned}$$

となり, 数学的帰納法から (5) が成り立つ. □

加法の単位元と同様, 乗法の単位元も 1 以外存在しない.

定理 9.6 (乗法の単位元の一意性). 自然数 $a \in \mathbb{N}$ が任意の自然数 $n \in \mathbb{N}$ に対して $n \cdot a = a \cdot n = n$ を満たせば $a = 1$ である.

Proof. n として 1 をとれば $1 \cdot a = a \cdot 1 = 1$ が成り立つ. 一方, 定理 11.3 の (2) より $a \cdot 1 = 1 \cdot a = a$ である. よって $a = 1$ が従う. □

9.4 半群とモノイド

数学の代数学という分野では, 集合に演算を定義し, その集合と演算の組 (**代数系**) の性質を調べていくことが基礎となっている. 今回定義した自然数の集合 $\mathbb{N}$ とその演算 $+$ や $\cdot$ の組 $(\mathbb{N}, +)$ と $(\mathbb{N}, \cdot)$ はどういった代数的構造を持つか紹介する.

集合 X に対し, 写像 $\circ: X \times X \rightarrow X$ を X 上の (二項) **演算** という. 例えば, $S = \{1, 2, 3\}$ とし, $X = 2^S$ とすれば, 和集合 $\cup$ は写像 $X \times X \rightarrow X, (A, B) \mapsto A \cup B$ と見なすことで X 上の演算となる. 一般に演算 $\circ$ の像は $\circ(a, b)$ ではなく $a \circ b$ と書く. $\circ$ の代わりに $+$ や $\cdot$ を考えるとわかりやすいだろう.

集合 X とその演算 $\circ$ に対し, $(X, \circ)$ が**半群** (semigroup) であるとは, $\circ$ に関して結合律

$$\forall x, y, z \in X, \quad x \circ (y \circ z) = (x \circ y) \circ z$$

が成り立つときにいう (結合律が成り立つと $x \circ y \circ z$ と書いても問題ない). つまり, $(\mathbb{N}, +)$ なら定理 9.3 の (4), $(\mathbb{N}, \cdot)$ なら定理 11.3 の (4) の性質のことである. よって $(\mathbb{N}, +)$ と $(\mathbb{N}, \cdot)$ はともに半群である.

$(X, \circ)$ を半群とする. このとき, 演算 $\circ$ に関する**単位元**とは

$$\forall x \in X, \quad x \circ a = a \circ x = x$$

を満たす元 $a \in X$ のことをいう. つまり, $(\mathbb{N}, +)$ なら 0, $(\mathbb{N}, \cdot)$ なら 1 のことである. 単位元を持つ半群のことを**モノイド** (monoid) と呼ぶ. よって $(\mathbb{N}, +)$ と $(\mathbb{N}, \cdot)$ はともにモノイドである. しかし, もし 0 が自然数ではないという定義を採用すれば, $(\mathbb{N}, +)$ はモノイドではなくなる. $(\mathbb{N}, \cdot)$ はいずれにしてもモノイドである.

半群やモノイドのイメージとしては, 「うまく足し算が定義された集合」が半群, それに加えて「0 のようなものがある」場合がモノイドである.

10 整数

前回の講義では、自然数の集合 $\mathbb{N}$ を公理を使って定義し、さらに加法 $+$ 、乗法 $\cdot$ の演算を定義し、それらの性質を調べた。その結果、普段から使っている自然数と、その中の加法と乗法は問題なく使用してよいことがわかった。今回の講義では、この自然数とその演算を使って整数を定義していく。

10.1 整数の定義

一旦、今まで使ってきた引き算を用いて、整数、特に負の整数がどう表されるか考える。例えば、 -2 は $1 - 3$ と 2 つの自然数の引き算で表すことができる。さらに、

$$-2 = 0 - 2 = 1 - 3 = 2 - 4 = \dots$$

と -2 を表す自然数の組は無限に存在する。このような $(0, 2), (1, 3), (2, 4), \dots$ という順序対を同一視してそれを -2 と対応させれば -2 は定義できそうである。同様に、どんな整数もこのように 2 つの自然数の組を使って定義できそうである。この同一視のため同値類を使う。それでは引き算を再び忘れて、整数を定義していく。直積集合 $\mathbb{N} \times \mathbb{N}$ 上の二項関係 $\sim$ を以下で定義する。

$$(n_1, m_1) \sim (n_2, m_2) \stackrel{\text{def}}{\iff} n_1 + m_2 = m_1 + n_2$$

右の等式は $n_1 - m_1 = n_2 - m_2$ を意味しているが、自然数の引き算は定義していないので、このように定義している。例えば、 $(0, 2) \sim (1, 3) \sim (2, 4)$ であることがわかるであろう。この $\sim$ は同値関係となる（小テストで確認）。すると $(0, 2), (1, 3), (2, 4)$ は「同じようなもの」として思えるのであった。ここで $\sim$ による同値類を考えてみると、

$$\begin{aligned} [(0, 0)]_{\sim} &= \{(0, 0), (1, 1), (2, 2), (3, 3), \dots\} && ((0, 0) \text{ を代表元とする同値類}) \\ [(1, 0)]_{\sim} &= \{(1, 0), (2, 1), (3, 2), (4, 3), \dots\} && ((1, 0) \text{ を代表元とする同値類}) \\ [(0, 1)]_{\sim} &= \{(0, 1), (1, 2), (2, 3), (3, 4), \dots\} && ((0, 1) \text{ を代表元とする同値類}) \\ [(2, 0)]_{\sim} &= \{(2, 0), (3, 1), (4, 2), (5, 3), \dots\} && ((2, 0) \text{ を代表元とする同値類}) \\ [(0, 2)]_{\sim} &= \{(0, 2), (1, 3), (2, 4), (3, 5), \dots\} && ((0, 2) \text{ を代表元とする同値類}) \end{aligned}$$

となっている。気持ちとして $[(n, m)]_{\sim}$ は整数 $n - m$ を表している。以降、単に $[(n, m)]$ と書く。この同値類のことを**整数**と呼ぶ。さらに整数全体の集合、つまり商集合 $\mathbb{N} \times \mathbb{N} / \sim$ を $\mathbb{Z}$ と書くことにする。また $[(0, 0)]$ を $\bar{0}$ 、 $[(1, 0)]$ を $\bar{1}$ 、 $[(0, 1)]$ を $\overline{-1}$ 、 $[(2, 0)]$ を $\bar{2}$ 、 $[(0, 2)]$ を $\overline{-2}, \dots$ のように書くこととする。すると

$$\mathbb{Z} = \{\bar{0}, \bar{1}, \overline{-1}, \bar{2}, \overline{-2}, \dots\}$$

となる。ここで上線をつけたのは自然数 $0, 1, 2, \dots$ と区別するためである。

10.2 整数の加法と乗法

自然数の加法と乗法を使って、整数の加法と乗法を定義する。実際、次のように定義する。

$$\begin{aligned} [(n_1, m_1)] +_{\mathbb{Z}} [(n_2, m_2)] &\stackrel{\text{def}}{=} [(n_1 + n_2, m_1 + m_2)] \\ [(n_1, m_1)] \cdot_{\mathbb{Z}} [(n_2, m_2)] &\stackrel{\text{def}}{=} [(n_1 \cdot n_2 + m_1 \cdot m_2, m_1 \cdot n_2 + n_1 \cdot m_2)] \end{aligned}$$

ここでは $\mathbb{N}$ 上の演算 $+$ や $\cdot$ と区別するために $+_{\mathbb{Z}}$ 、 $\cdot_{\mathbb{Z}}$ と書いている。これは $1 + 1$ と $\bar{1} + \bar{1}$ は違う意味であることを強調するためである。ただし以降は単に $+$ 、 $\cdot$ と書く。なぜこのように定義するかというと、これまで使ってきた引き算に対し、2 つの整数 $n_1 - m_1$ と $n_2 - m_2$ の和と積を考えると、

$$\begin{aligned} (n_1 - m_1) + (n_2 - m_2) &= (n_1 + n_2) - (m_1 + m_2) \\ (n_1 - m_1) \cdot (n_2 - m_2) &= (n_1 n_2 + m_1 m_2) - (m_1 n_2 + n_1 m_2) \end{aligned}$$

となっているからである．具体的に計算してみると，

$$\overline{-2} \cdot \overline{3} = [(0, 2)] \cdot [(3, 0)] = [(0 \cdot 3 + 2 \cdot 0, 3 \cdot 2 + 0 \cdot 0)] = [(0, 6)] = \overline{-6}$$

となる．これで整数の加法と乗法が定義できたと思えるが，実は商集合での演算は確認しないといけないことがある．それが **well-defined 性** である．日本語で無理やり訳すなら「矛盾なく定義される」ということである．上の演算では同値類 $[(n, m)]$ の (n, m) という代表元の情報を使っている．しかし，例えば $[(0, 2)] = [(1, 3)] = [(2, 4)] = \dots$ のように代表元は取り替えることが可能である．上の演算で確かめられないのは，「代表元の取り方を変えても，その演算の結果は変わらない」ということである．例えば，

$$[(0, 2)] + [(1, 0)] = [(1, 2)] = [(2, 3)] = [(1, 3)] + [(1, 0)]$$

であり， $[(0, 2)]$ を $[(1, 3)]$ に取り替えても演算の結果は同じである．

well-defined ではないものは少し想像しにくいと思うので，例を少し見てみよう．一旦，分数を普段使っているものだと思い，分数の演算を

$$\frac{m_1}{n_1} \star \frac{m_2}{n_2} = \frac{m_1 + m_2}{n_1 + n_2}$$

として定義する（よくある間違った分数の足し算である）．このとき， $\frac{1}{3} \star \frac{1}{2} = \frac{2}{5}$ となる．しかし，我々は $\frac{1}{3} = \frac{2}{6}$ であることを知っているので $\frac{1}{3}$ を $\frac{2}{6}$ に取り替えても演算の結果が同じにならないとおかしい．ところが， $\frac{2}{6} \star \frac{1}{2} = \frac{3}{8}$ であり， $\frac{3}{8} \neq \frac{2}{5}$ となるため，演算の結果が変わってしまう．実は分数は同値類を使って表される（次回定義）が， $\frac{1}{3}$ を $\frac{2}{6}$ に取り替えることは，代表元を取り替えていることに対応している．つまり，上の演算は代表元の取り方を変えると演算の結果が変わってしまうことになり，この演算は well-defined ではないということになる．

それでは上で定義した整数の演算が well-defined であることを証明する．

定理 10.1. 整数の加法と乗法は well-defined である．

Proof. 加法のみを証明する．任意の $(n_1, m_1), (n'_1, m'_1), (n_2, m_2), (n'_2, m'_2) \in \mathbb{N} \times \mathbb{N}$ で $(n_1, m_1) \sim (n'_1, m'_1)$ かつ $(n_2, m_2) \sim (n'_2, m'_2)$ となるものを取る．このとき，

$$n_1 + m'_1 = m_1 + n'_1, \quad n_2 + m'_2 = m_2 + n'_2 \quad (\#)$$

である．示したいことは

$$[(n_1, m_1)] + [(n_2, m_2)] = [(n_1 + n_2, m_1 + m_2)] = [(n'_1 + n'_2, m'_1 + m'_2)] = [(n'_1, m'_1)] + [(n'_2, m'_2)]$$

である，つまり

$$(n_1 + n_2, m_1 + m_2) \sim (n'_1 + n'_2, m'_1 + m'_2)$$

を示せば良い．実際，これは

$$(n_1 + n_2) + (m'_1 + m'_2) = (n_1 + m'_1) + (n_2 + m'_2) \stackrel{(\#)}{=} (n'_1 + m_1) + (n'_2 + m_2) = (m_1 + m_2) + (n'_1 + n'_2)$$

より従う（使っているのは自然数の加法の性質と $(\#)$ のみである）．よって加法の結果は代表元の取り方に依存しないので加法は well-defined である． $\square$

次に，上で定義した整数の加法と乗法は，自然数の加法と乗法と同様の性質を満たす（証明は省略する）．

定理 10.2 (整数の加法の性質). 任意の整数 $\bar{x}, \bar{y}, \bar{z} \in \mathbb{Z}$ に対し，以下が成り立つ．

1. $\bar{x} + (\bar{y} + \bar{z}) = (\bar{x} + \bar{y}) + \bar{z}$ (加法の結合律)．
2. $\bar{x} + \bar{0} = \bar{0} + \bar{x} = \bar{x}$ (加法の単位元)．
3. $\bar{x} + \bar{y} = \bar{y} + \bar{x}$ (加法の交換律)．

定理 10.3 (整数の乗法の性質). 任意の整数 $\bar{x}, \bar{y}, \bar{z} \in \mathbb{Z}$ に対し, 以下が成り立つ.

1. $(\bar{x} \cdot \bar{y}) \cdot \bar{z} = \bar{x} \cdot (\bar{y} \cdot \bar{z})$ (乗法の結合律).
2. $\bar{x} \cdot \bar{1} = \bar{1} \cdot \bar{x} = \bar{x}$ (乗法の単位元).
3. $\bar{x} \cdot \bar{0} = \bar{0} \cdot \bar{x} = \bar{0}$.
4. $\bar{x} \cdot \bar{y} = \bar{y} \cdot \bar{x}$ (乗法の交換律).
5. $\bar{x} \cdot (\bar{y} + \bar{z}) = \bar{x} \cdot \bar{y} + \bar{x} \cdot \bar{z}, (\bar{x} + \bar{y}) \cdot \bar{z} = \bar{x} \cdot \bar{z} + \bar{y} \cdot \bar{z}$ (分配律).

定理 10.4 (加法と乗法の単位元の一意性). 整数 $\bar{a} \in \mathbb{Z}$ が任意の整数 $\bar{x} \in \mathbb{Z}$ に対し, $\bar{a} + \bar{x} = \bar{x} + \bar{a} = \bar{x}$ を満たせば $\bar{a} = \bar{0}$ である. 一方, $\bar{a} \cdot \bar{x} = \bar{x} \cdot \bar{a} = \bar{x}$ を満たせば $\bar{a} = \bar{1}$ である.

10.3 整数の減法

自然数と違い, 整数の引き算は再び整数であったことを思い出そう. したがって加法と同様に減法を定義することができる. しかし今回は, 「引き算」の意義を踏まえて定義していくことにする. 一旦整数の加法に戻り, 自然数の場合には成り立たなかった性質を証明する.

定理 10.5 (加法の逆元の存在). 任意の整数 $\bar{x} \in \mathbb{Z}$ に対し, $\bar{a} + \bar{x} = \bar{x} + \bar{a} = \bar{0}$ を満たす整数 $\bar{a} \in \mathbb{Z}$ がただ 1 つ存在する.

Proof. $\bar{x} = [(n, m)]$ とする. このとき, $\bar{a} = [(m, n)]$ とすると,

$$\bar{x} + \bar{a} = [(n + m, m + n)] = [(n + m, n + m)] = [(0, 0)] = \bar{0}$$

かつ

$$\bar{a} + \bar{x} = [(m + n, n + m)] = [(n + m, n + m)] = [(0, 0)] = \bar{0}$$

が言えるので条件を満たす $\bar{a}$ は存在する. このような $\bar{a}$ がただ 1 つしか存在しないことを示す. もし $\bar{b} \in \mathbb{Z}$ が $\bar{b} + \bar{x} = \bar{x} + \bar{b} = \bar{0}$ を満たすとき,

$$\bar{a} = \bar{a} + \bar{0} = \bar{a} + (\bar{x} + \bar{b}) = (\bar{a} + \bar{x}) + \bar{b} = \bar{0} + \bar{b} = \bar{b}$$

となり, 条件を満たす $\bar{a}$ はただ 1 つしか存在しない. □

整数 $\bar{x} \in \mathbb{Z}$ に対し, $\bar{a} + \bar{x} = \bar{x} + \bar{a} = \bar{0}$ を満たす整数 $\bar{a} \in \mathbb{Z}$ を $\bar{x}$ の加法に関する**逆元**といい, $-\bar{x}$ と書くことにする. このとき $\overline{-1}$ と $-\bar{1}$ に現れる「 $-$ 」という記号はそれぞれ定義が違うが結局は同じ意味となる. 実際, $\bar{x} = [(n, m)]$ とする. すると定理の証明から, $-\bar{x}$ の「 $-$ 」という記号は $\bar{x}$ の代表元の成分の順番を入れ替える操作を意味する. よって $-\bar{1} = -[(1, 0)] = [(0, 1)] = \overline{-1}$ や $-(\overline{-1}) = -[(0, 1)] = [(1, 0)] = \bar{1}$ となることになる.

それでは減法を定義しよう. 整数の減法は加法の逆元との足し算で定義される. つまり

$$\bar{x} -_{\text{def}} \bar{y} = \bar{x} + (-\bar{y})$$

である. したがって減法の性質は加法の性質から導かれるので, 2 つの演算を別々に考える必要はない. 結局, 「引き算ができる」というのは「加法に関する逆元がいつでも存在する」ということに他ならない. 代数学では後者の性質が重要となる.

次に符号に関する話をする. 中学校で負の数が登場した時, 「マイナス」×「マイナス」=「プラス」, 「マイナス」×「プラス」=「マイナス」というルールで負の数の掛け算を習ったであろう. これは中学校での負の数の定義が曖昧だったために仕方がなく認めたルールである. しかし, 「マイナス」を「加法に関する逆元を表す記号」として定義するとこのルールが証明できる.

定理 10.6. 任意の整数 $\bar{x}, \bar{y} \in \mathbb{Z}$ に対し、以下が成り立つ。

$$1. (-\bar{x}) \cdot \bar{y} = \bar{x} \cdot (-\bar{y}) = -(\bar{x} \cdot \bar{y}).$$

$$2. (-\bar{x}) \cdot (-\bar{y}) = \bar{x} \cdot \bar{y}.$$

Proof. (1) まず $-(\bar{x} \cdot \bar{y}) = (-\bar{x}) \cdot \bar{y}$ を示す。この式を日本語で説明すると「 $\bar{x} \cdot \bar{y}$ は $(-\bar{x}) \cdot \bar{y}$ の加法に関する逆元である」ということである。さらに言い直すと「 $\bar{x} \cdot \bar{y}$ と $(-\bar{x}) \cdot \bar{y}$ の和は $\bar{0}$ である」ということになる。これは

$$\bar{x} \cdot \bar{y} + ((-\bar{x}) \cdot \bar{y}) = (\bar{x} + (-\bar{x})) \cdot \bar{y} = \bar{0} \cdot \bar{y} = \bar{0}$$

より成り立つ。 $\bar{x} \cdot (-\bar{y}) = -(\bar{x} \cdot \bar{y})$ も同様に示せる。

(2) 次の式変形により示せる。

$$\begin{aligned} \bar{x} \cdot \bar{y} &= \bar{x} \cdot \bar{y} + \bar{0} = \bar{x} \cdot \bar{y} + (-\bar{x}) \cdot \bar{0} = \bar{x} \cdot \bar{y} + ((-\bar{x}) \cdot (\bar{y} + (-\bar{y}))) \\ &= \bar{x} \cdot \bar{y} + ((-\bar{x}) \cdot \bar{y} + (-\bar{x}) \cdot (-\bar{y})) = (\bar{x} \cdot \bar{y} + (-\bar{x}) \cdot \bar{y}) + (-\bar{x}) \cdot (-\bar{y}) \\ &= (\bar{x} \cdot \bar{y} + (-\bar{x} \cdot \bar{y})) + (-\bar{x}) \cdot (-\bar{y}) = \bar{0} + (-\bar{x}) \cdot (-\bar{y}) = (-\bar{x}) \cdot (-\bar{y}). \end{aligned}$$

□

10.4 群と環

$\mathbb{Z}$ の代数的構造を見ていこう。減法の定義のところで説明したとおり、逆元の存在は代数系にとって非常に重要である。半群やモノイドよりさらに特別な代数系を紹介する。

$(X, \circ)$ をモノイドとし、元 $e \in X$ を X の $\circ$ に関する単位元、つまり任意の $x \in X$ に対し $e \circ x = x \circ e = x$ を満たす元とする。元 $a \in X$ に対し、 $a \circ b = b \circ a = e$ を満たす元 $b \in X$ のことを、 a の演算 $\circ$ に関する**逆元**という。逆元は存在すれば一意である（証明は定理 10.5 の後半と同様）。モノイド $(X, \circ)$ が**群** (group) であるとは、任意の $x \in X$ が $\circ$ に関して逆元をもつときにいう。特に、交換律、つまり任意の $x, y \in X$ に対して $x \circ y = y \circ x$ を満たす群を**アーベル群** (abelian group) または**加法群** (additive group) という。 $(\mathbb{N}, +)$, $(\mathbb{N}, \cdot)$, $(\mathbb{Z}, +)$, $(\mathbb{Z}, \cdot)$ の中で $(\mathbb{Z}, +)$ のみがアーベル群であり、それ以外は群ですらない。実際、 $\mathbb{N}$ の中で $1 + x = x + 1 = 0$ を満たす $x \in \mathbb{N}$ は存在しないし、 $\mathbb{Z}$ の中で $\bar{2} \cdot \bar{x} = \bar{x} \cdot \bar{2} = \bar{1}$ を満たす $\bar{y} \in \mathbb{Z}$ は存在しない。つまり、それぞれの演算に関して逆元が常に存在するとは限らないのである。

ここまでの代数系は、集合と 1 つの演算の組を考えていたが、より細かい代数構造として加法と乗法を同時に扱うことが多い。集合 X に対し、加法 $+$ と乗法 $\cdot$ が定義されているとする。このとき、3 つ組 $(X, +, \cdot)$ が**環** (ring) であるとは、 $(X, +)$ がアーベル群かつ $(X, \cdot)$ がモノイドであり、さらに分配律

$$x \cdot (y + z) = x \cdot y + x \cdot z, (x + y) \cdot z = x \cdot z + y \cdot z, \forall x, y, z \in X$$

が成り立つときにいう。特に、 $\cdot$ に関して交換律が成り立てば**可換環** (commutative ring) という。よって $(\mathbb{Z}, +, \cdot)$ は可換環である。 $(\mathbb{N}, +, \cdot)$ は $(\mathbb{N}, +)$ が群ではないので、環とはならない。また可換ではない環（非可換環）の例は、2 次正方行列全体の集合とその加法と乗法を考えればよい。

半群、群、環のイメージとしては、「足し算」が定義できる集合が半群、「足し算と引き算」が定義できる集合が群、「足し算と引き算と掛け算」が定義できる集合が環である。代数系を研究する理由は複数の対象を統一的に扱えることである。例えば、素因数分解の一意性と多項式の因数分解の一意性は、整数の集合と多項式の集合がそれぞれ**一意分解整域**と呼ばれる特別な環になることから従う。また「ルービックキューブを解く」ことは群を使って説明できたり、暗号理論の研究では環の研究が重要になってくる。

11 有理数

前回の講義では、自然数と同値類を用いて整数を定義し、そして整数上の加法、乗法を定義した。また減法は加法に関する逆元の足し算を考えることで定義できた。今回の講義では、さらに拡張し、有理数を定義し、その性質を調べる。ただし、証明方法はこれまでとほぼ同じ流れなので、新しいこと以外は省略する。

11.1 有理数の定義

ここでは整数は通常通り $0, 1, -1, 2, -2, \dots$ と書き、これまで通りの加法、減法、乗法を使う。整数のときと同様に、有理数の定義でも同値類を用いる。整数を有理数に拡張するということは、結局、「整数上の分数」を定義することである。「小数」という概念はここでは考えない。例えば、 $\frac{2}{3}$ は分子 2 と分母 3 の 2 つの整数の組でできている。整数のときと同様で、

$$\frac{2}{3} = \frac{-2}{-3} = \frac{4}{6} = \frac{-4}{-6} = \dots$$

のように $\frac{2}{3}$ を表す分数（整数の組）は無限個存在する。0 が分母に現れなかったことに注意し、有理数を定義しよう。 $\mathbb{Z}$ を整数全体の集合とし、 $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$ で 0 以外の整数全体の集合を表すことにする。直積集合 $\mathbb{Z} \times \mathbb{Z}^*$ 上の二項関係 $\sim$ を以下で定義する。

$$(p_1, q_1) \sim (p_2, q_2) \stackrel{\text{def}}{\Leftrightarrow} p_1 \cdot q_2 = p_2 \cdot q_1$$

ここでの演算「 $\cdot$ 」は整数上の乗法である。例えば、 $(2, 3) \sim (-2, -3) \sim (4, 6) \sim (-4, -6)$ であることがわかるであろう。この $\sim$ は同値関係である（各自確認）。ここで $\sim$ による同値類を考えてみると、

$$[(0, 1)]_{\sim} = \{(0, 1), (0, -1), (0, 2), (0, -2), \dots\} \quad ((0, 1) \text{ を代表元とする同値類})$$

$$[(1, 1)]_{\sim} = \{(1, 1), (-1, -1), (2, 2), (-2, -2), \dots\} \quad ((1, 1) \text{ を代表元とする同値類})$$

$$[(-1, 1)]_{\sim} = \{(-1, 1), (1, -1), (-2, 2), (2, -2), \dots\} \quad ((-1, 1) \text{ を代表元とする同値類})$$

$$[(1, 2)]_{\sim} = \{(1, 2), (-1, -2), (2, 4), (-2, -4), \dots\} \quad ((1, 2) \text{ を代表元とする同値類})$$

となっている。気持ちとして $[(p, q)]_{\sim}$ は分数 $\frac{p}{q}$ を表している。以降、単に $[(p, q)]$ と書く。この同値類 $[(p, q)]$ を**有理数**と呼ぶ。さらに、有理数全体の集合、つまり商集合 $(\mathbb{Z} \times \mathbb{Z}^*) / \sim$ を $\mathbb{Q}$ と書くことにする。また $[(p, q)]$ を $\frac{p}{q}$ で略記することで、

$$\frac{4}{6} = [(4, 6)] = [(2, 3)] = \frac{2}{3}$$

のように約分することができる。ここで、2 と $\frac{2}{1}$ は違う集合に属することに注意しよう。これは $\mathbb{Z}$ の元と $\mathbb{Q}$ の元を区別するためである。

11.2 有理数の加法、乗法

次に有理数の加法と乗法を定義する。実際、次のように定義する。

$$[(p_1, q_1)] +_{\mathbb{Q}} [(p_2, q_2)] \stackrel{\text{def}}{=} [(p_1 \cdot q_2 + p_2 \cdot q_1, q_1 \cdot q_2)]$$

$$[(p_1, q_1)] \cdot_{\mathbb{Q}} [(p_2, q_2)] \stackrel{\text{def}}{=} [(p_1 \cdot p_2, q_1 \cdot q_2)]$$

以降 $+_{\mathbb{Q}}$ と $\cdot_{\mathbb{Q}}$ は単に $+$ と $\cdot$ と書く。なぜこのように定義するかというと、これまで使ってきた分数の足し算と掛け算を考えると、

$$\begin{aligned} \frac{p_1}{q_1} + \frac{p_2}{q_2} &= \frac{p_1 q_2 + p_2 q_1}{q_1 q_2} \\ \frac{p_1}{q_1} \cdot \frac{p_2}{q_2} &= \frac{p_1 p_2}{q_1 q_2} \end{aligned}$$

となっているからである．具体的に計算してみると，

$$\frac{1}{6} + \frac{2}{3} = [(1, 6)] + [(2, 3)] = [(1 \cdot 3 + 2 \cdot 6, 6 \cdot 3)] = [(15, 18)] = [(5, 6)] = \frac{5}{6}$$

となる．

整数のときと同様で，この演算が well-defined であることを確認する必要がある．

定理 11.1. 有理数の加法，乗法は well-defined である．

次に，上で定義した有理数の演算の性質をそれぞれ見ていく．便宜上 $\mathbf{0} = \frac{0}{1}$ と書くことにする．

定理 11.2 (有理数の加法の性質)．任意の有理数 $x, y, z \in \mathbb{Q}$ に対し，以下が成り立つ．

1. $x + (y + z) = (x + y) + z$ (加法の結合律)．
2. $x + y = y + x$ (加法の交換律)．
3. $x + \mathbf{0} = \mathbf{0} + x = x$ (加法の単位元)．
4. $x + a = a + x = \mathbf{0}$ を満たす有理数 $a \in \mathbb{Q}$ がただ 1 つ存在する (加法の逆元の存在)．

(4) の a は $x = [(p, q)]$ に対し， $a = [(-p, q)]$ とすればよい． x の加法に関する逆元を $-x$ と書くこととすると，有理数の減法は

$$x -_{\mathbb{Q}} y \stackrel{\text{def}}{=} x + (-y)$$

と定義すればよい．

次に有理数の乗法の性質を見ていく．便宜上， $\mathbf{1} = \frac{1}{1}$ と書くことにする．

定理 11.3 (有理数の乗法の性質)．任意の有理数 $x, y, z \in \mathbb{Q}$ に対し，以下が成り立つ．

1. $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ (乗法の結合律)．
2. $x \cdot y = y \cdot x$ (乗法の交換律)．
3. $x \cdot \mathbf{1} = \mathbf{1} \cdot x = x$ (乗法の単位元)．
4. $\mathbf{0} \cdot x = x \cdot \mathbf{0} = \mathbf{0}$ ．
5. $x \cdot (y + z) = x \cdot y + x \cdot z$, $(x + y) \cdot z = x \cdot z + y \cdot z$ (分配律)．

また整数のときと同様で符号の掛け算も確認できる．

定理 11.4. 任意の有理数 $x, y \in \mathbb{Q}$ に対し，以下が成り立つ．

1. $(-x) \cdot y = x \cdot (-y) = -(x \cdot y)$ ．
2. $(-x) \cdot (-y) = x \cdot y$ ．

11.3 有理数の除法

整数の場合，乗法に関する逆元は 1 と -1 の場合にしか存在しなかった．しかし，有理数の場合，ほとんどすべての元 に対し，乗法に関する逆元が存在する．

定理 11.5 (乗法の逆元の存在)． $\mathbf{0}$ を除く任意の有理数 $x \in \mathbb{Q} \setminus \{\mathbf{0}\}$ に対し，

$$x \cdot y = y \cdot x = \mathbf{1}$$

を満たす有理数 $y \in \mathbb{Q}$ がただ 1 つ存在する．

Proof. $x = [(p, q)] \in \mathbb{Q} \setminus \{0\}$ とする. このとき, $p, q \neq 0$ であるので, $[(q, p)] \in \mathbb{Q}$ が存在し, それを y とすると,

$$x \cdot y = [(p \cdot q, p \cdot q)] = [(1, 1)] = \mathbf{1}$$

であり, 条件を満たす $y \in \mathbb{Q}$ が存在する.

一意性を示す. $z \in \mathbb{Q}$ が $x \cdot z = z \cdot x = \mathbf{1}$ を満たすとする. このとき,

$$z = z \cdot \mathbf{1} = z \cdot (x \cdot y) = (z \cdot x) \cdot y = \mathbf{1} \cdot y = y$$

より, 一意性は示された. □

一方, 定理 11.3 の (4) より, $\mathbf{0}$ は乗法に関して逆元を持たない. $\mathbf{0}$ ではない有理数 $x \in \mathbb{Q} \setminus \{0\}$ の乗法に関する逆元を x^{-1} と書くことにする. つまり, $x = [(p, q)]$ ならば $x^{-1} = [(q, p)]$ である. $-x$ の「 $-$ 」がただの記号であったように, x^{-1} の「 -1 」は -1 という整数ではなく, ただの記号である. 乗法の逆元の性質から

$$(x^{-1})^{-1} = x$$

であることがわかる. 先ほど述べたように「 -1 」は記号であったので, 指数法則を使って $(-1) \cdot (-1) = 1$ と計算しているわけではない. この等式は「 x^{-1} の乗法に関する逆元は x である」ということを述べているに過ぎないことに注意しよう.

さて, 減法は加法の逆元の足し算で定義することができた. 同じ考えで, 除法は乗法の逆元の掛け算で定義される. つまり, 有理数 $x, y \in \mathbb{Q}$ で $y \neq \mathbf{0}$ となるものに対し, 有理数の除法を次のように定義する:

$$x \div_{\mathbb{Q}} y \stackrel{\text{def}}{=} x \cdot y^{-1}.$$

具体的に計算してみると

$$\frac{1}{6} \div \frac{2}{3} = [(1, 6)] \div [(2, 3)] = [(1, 6)] \cdot [(2, 3)]^{-1} = [(1, 6)] \cdot [(3, 2)] = [(1 \cdot 3, 6 \cdot 2)] = [(3, 12)] = [(1, 4)] = \frac{1}{4}$$

となる.

このように定義すると「なぜ $\mathbf{0}$ で割れないのか?」という疑問は「 $\mathbf{0}$ は乗法に関する逆元を持たないから」と理由づけることができる.

11.4 体

有理数の集合は四則演算 (足し算, 引き算, 掛け算, 割り算) がうまく定義されていることがわかった. こういった代数系を体 (たい) という. 集合 X と X 上の演算 $+$ と $\cdot$ に対し, $(X, +, \cdot)$ が**体 (field)** であるとは, $(X, +, \cdot)$ が可換環でかつ, 性質「 $+$ に関する単位元 ($\mathbf{0}$ のこと) を除いて, 全ての元は $\cdot$ に関して逆元を持つ」を満たすときにいう. この後ろの性質が「割り算が定義できる」ということである. $\mathbb{Q}$ のことを**有理数体 (rational field)** と呼び, 計算機やプログラミングにおける一般的な「数」として扱われる. これまで登場した「群・環・体」が代数学の基本的な研究対象 (道具) である.

11.5 有理数上の順序

これまで自然数から始めて, 整数, 有理数と定義してきたが, まだその中の数の順序を定義していない. 再び自然数から順序関係を定義していく. 整数と有理数では同値関係を使って定義していたので, 区別するために, 整数を定義するときに使う同値関係を $\sim_{\mathbb{Z}}$, 有理数を定義するときに使う同値関係を $\sim_{\mathbb{Q}}$ と書く. また各演算も $+\mathbb{N}, +\mathbb{Z}, +\mathbb{Q}$ のように書く. 自然数 $x, y \in \mathbb{N}$ に対し, $\mathbb{N}$ 上の関係を

$$x \leq_{\mathbb{N}} y \stackrel{\text{def}}{\iff} y = x +_{\mathbb{N}} a \text{ となる, ある自然数 } a \in \mathbb{N} \text{ が存在する}$$

で定義する．つまり y は x と同じか， x のいくつか後ろの自然数である．すると $\leq_{\mathbb{N}}$ は順序関係となる．次に，整数 $[(n_1, m_1)]_{\sim_{\mathbb{Z}}}, [(n_2, m_2)]_{\sim_{\mathbb{Z}}} \ (n_1, n_2, m_1, m_2 \in \mathbb{N})$ に対し， $\mathbb{Z}$ 上の関係を

$$[(n_1, m_1)]_{\sim_{\mathbb{Z}}} \leq_{\mathbb{Z}} [(n_2, m_2)]_{\sim_{\mathbb{Z}}} \stackrel{\text{def}}{\iff} n_1 +_{\mathbb{N}} m_2 \leq_{\mathbb{N}} m_1 +_{\mathbb{N}} n_2$$

で定義する．これは $n_1 - m_1 \leq n_2 - m_2$ が $n_1 + m_2 \leq m_1 + n_2$ と同値であることから導かれる． $\leq_{\mathbb{Z}}$ の定義の中で $\leq_{\mathbb{N}}$ を使っていることも注意が必要である（定義する前までは自然数の順序関係しかないため）．このとき $\leq_{\mathbb{Z}}$ は well-defined であり，さらに順序関係である．最後に，有理数上の順序のために，正の整数の集合 $\mathbb{Z}^+ = \{a \in \mathbb{Z} : a >_{\mathbb{Z}} 0\}$ を考える．このとき，どんな有理数 $x \in \mathbb{Q}$ も代表元を $(p, q) \in \mathbb{Z} \times \mathbb{Z}^+$ からとってこれる．つまり，分母を正の整数とすることができる．すると有理数 $[(p_1, q_1)]_{\sim_{\mathbb{Q}}}, [(p_2, q_2)]_{\sim_{\mathbb{Q}}} \ (p_1, p_2 \in \mathbb{Z}, q_1, q_2 \in \mathbb{Z}^+)$ に対し， $\mathbb{Q}$ 上の関係を

$$[(p_1, q_1)]_{\sim_{\mathbb{Q}}} \leq_{\mathbb{Q}} [(p_2, q_2)]_{\sim_{\mathbb{Q}}} \stackrel{\text{def}}{\iff} p_1 \cdot_{\mathbb{Z}} q_2 \leq_{\mathbb{Z}} p_2 \cdot_{\mathbb{Z}} q_1$$

で定義する．これは $q_1, q_2 > 0$ から， $\frac{p_1}{q_1} \leq \frac{p_2}{q_2}$ と $p_1 q_2 \leq p_2 q_1$ が同値であることから導かれる．このとき $\leq_{\mathbb{Q}}$ は well-defined であり，さらに順序関係である．

以上より，自然数，整数，有理数の順序関係を定義することができた．特に，上記の順序関係が全順序であることも証明できる．情報数理 A で勉強した濃度を考えると， $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ は同じ濃度であった．つまり無限集合としてこの 3 つの集合の「大きさ」は同じである．しかし，順序集合で見ると，有理数は他の 2 つに比べると「びっしりつまっている」性質を持つ．実際，

定理 11.6. 任意の異なる有理数 $a, b \in \mathbb{Q}$ （ただし $a <_{\mathbb{Q}} b$ ）に対し， $a <_{\mathbb{Q}} c <_{\mathbb{Q}} b$ となる有理数 $c \in \mathbb{Q}$ が存在する．

証明は通常の有理数と通常の演算を考え， c として a と b の平均（中間値）を取ればよい．この性質は自然数と整数では成り立たないことはわかるであろう（例えば 1 と 2）．この性質を有理数の**稠密性**という．

11.6 実数と複素数

我々が普段使っている「数」は実数であろうが，実数の集合 $\mathbb{R}$ を定義するにはさらなる道具が必要である．少し大雑把に紹介する．実数の一般的な構成法は有理数の集合 $\mathbb{Q}$ の**完備化**である．これは**コーシー列**と呼ばれる後ろの方ではほとんど動かない数列を定義し，そのコーシー列にある同値関係を入れ，その同値類を実数とする方法である．もう一つの方法は**デデキント切断**という有理数の集合 $\mathbb{Q}$ を 2 つの集合 A と B で $(a, b) \in A \times B$ なら $a \leq b$ となるように分ける方法 (A, B) を実数とする方法である．興味がある人は自分で調べてみてほしい．実数が定義できれば，複素数の集合 $\mathbb{C}$ 定義は簡単である． $a + b\sqrt{-1}$ という複素数を実数の組 $(a, b) \in \mathbb{R}^2$ と対応させて，加法と乗法を

$$\begin{aligned} (a_1, b_1) +_{\mathbb{C}} (a_2, b_2) &= (a_1 + a_2, b_1 + b_2) \\ (a_1, b_1) \cdot_{\mathbb{C}} (a_2, b_2) &= (a_1 a_2 - b_1 b_2, a_1 b_2 + a_2 b_1) \end{aligned}$$

と定義すればいいだけである（これは初回の授業で考えた問題である）．こうすれば， $\sqrt{-1} \cdot \sqrt{-1} = -1$ となっている．実数や複素数も体となっていて，それぞれ**実数体** (real field) と**複素数体** (complex field) と呼ぶ．この 2 つの体の大きな違いは複素数体の場合，どんな n 次多項式も重複を含めて n 個の解を持つということである（代数学の基本定理）．こういった性質を持つ体を**代数閉体** (algebraic closed field) と呼ぶ．