$1+1=2$ と $(-1)\times(-1)=1$ の証明

カプースタ　(Twitter：@s3tudyroom)

目 次

第1章　$1+1$が2であることについて

誰もが一度は「なぜ$1+1$は2になるのか」と疑問に思ったことがあるだろう．今回はこの疑問を解決させたいと思う.「そう決めたから」と言ってしまえばそれまでなのだが，これでは納得できない人もいるだろう．実際,「そう決めた」というにはあまりに長い考察が必要になる．今回はどんな考察が必要なのか紹介しようと思う．

“$1+1=2$”を示すためには，まず，記号の意味を理解する必要がある．この数式に登場する記号は“1”,“2”,“$+$”,“$=$”の4つである．このうち“$=$”はこの記号の左右にある記号が“同じもの”であることを表すものとする．ここでは“$=$”についてこれ以上厳密な事は議論しないことにする．残りの3つの記号については，これから定義していく．

この章では，“1”,“2”は自然数として考えて定義していく．なぜこんなことを断るのかというと，自然数から整数や有理数を定義すると，定義上は整数，有理数に自然数としての“1”,“2”は含まれなくなるから，注意が必要なのである．

大まかな証明の流れは，自然数を定義して，その元として記号“1”,“2”を定める．そして，自然数上の二項演算“加法”を定義し，その二項演算子として記号“$+$”を導入する．ここでようやく“$1+1$”が議論でき，それが“2”と“同じもの”であることを示して証明終了である．

1.1　自然数の定義

まず，自然数が何であるかを定義していく．ここで“自然数全体の集合$\mathbb{N}$”は“Peanoの公理を満たす集合”であると定義する．なお，自然数に0を含めるかどうかについては，どちらの考え方もあるが，今回0は自然数に含めることにする．

1.1.1　Peanoの公理

【Peanoの公理】
集合NがPeanoの公理を満たすとは，集合Nの元0と単射$\sigma : N \to N$があり，次の2つの条件を満たすことである．

(N1)　$\forall n \in N, \sigma(n) \neq 0$

(N2)　Nの任意の部分集合Sについて

$$0 \in S \text{ かつ} \sigma(S) \subset S \Longrightarrow S = N$$

ここで，集合Nの元0は，我々の思っている日常的な意味での数“0”であると（少なくとも今は）考えてはいけないことを注意しておく．なぜなら，今我々は自然数を定義しようとしているため，自然数自体，特に日常的に使っている数“0”を知らないのである．なのでここでの“0”は，集合Nの中に特別な（条件(N1)を満たす）元“0”があるというぐらいに思っているとよい．

1.1.2 Peano の公理の直感的な意味

ここで，Peano の公理の直感的な意味を書いておく．集合 N の元 0 があるとは，上で述べた通り，集合 N の中に特別な元 0 があるということだ．単射 $\sigma : N \to N$ は，後者関数とも呼ばれ，$\sigma(n)$ を n の後者と言ったりする．

条件 (N1) は元 0 が自然数の“始まり”であることを意味している．さらには，0 が自然数の中で最小となることである．しかしこれは，自然数の大小関係は定義してないので，あまり意味を持たない．これが意味を持つのは，我々の普段使っている自然数の大小関係を順序関係として（単射 σ を用いて）定義したときのことであるが，今回は“$1+1=2$”を導くことが目的なので，自然数の順序関係には触れない．

条件 (N2) は数学的帰納法の原理である．実際，条件 (N2) によって，数学的帰納法が使えることが証明できる．しかし，これも目的とは関係ないので触れないことにする．興味がある人のために，そのとき証明する命題を書いておくので，証明してみるとよい．

【数学的帰納法】
任意の自然数 n について命題 $P(n)$ があり，次が成り立つとする．

(1) $P(0)$ は正しい
(2) $P(n)$ が正しいなら $P(n+1)$ も正しい

このとき，すべての自然数 n について $P(n)$ は正しい．
また，これを利用した証明の方法を数学的帰納法という．

ここで，$n+1$ という記号を使ったが，今はまだ定義していない．これは後々定義するので，そのときの定義からこの命題を証明しなくてはならないことを注意しておく．

1.1.3 “Peano の公理を満たす集合”の本質的な一意性

これで，“自然数全体の集合 $\mathbb{N}$”が定義できたと安心してはならない．このままでは，“Peano の公理を満たす集合”が本質的に複数ある可能性があるからだ．これは，非常に深刻な問題である．“Peano の公理を満たす集合”が本質的に複数あると，“自然数全体の集合 $\mathbb{N}$”が 1 つに定まらないことになる．

なのでここから，今回の議論において最も重要な定理として，2 つの“Peano の公理を満たす集合” N, N' が本質的に同じ集合になることを示す．ここで，2 つの“Peano の公理を満たす集合” N, N' が本質的に同じ集合であるとは，N から N' への全単射がただ 1 つ存在し，それぞれの Peano の公理という性質が失われないということである．つまり，“0”同士が対応し，“単射 σ”が保存されることである．これを示すべき定理として明記しておく．

【定理 1.1】
2 つの集合 N, N' と，それらの集合の元 $0, 0'$，単射 σ, σ' があり，これらは Peano の公理を満たすとする．このとき，次の条件を満たす全単射 $f : N \to N'$ がただ 1 つ存在する．

(i) $f(0) = 0'$
(ii) $f \circ \sigma = \sigma' \circ f$

今我々は新しい概念として自然数を定義しようとしているので，この定理さえ満たせば 2 つの集合 N と N' を区別する必要がなくなる．これで，“自然数全体の集合 $\mathbb{N}$”が定義できるようになる．

この定理 1.1 をこれから証明していくにあたって，以降集合 N は Peano の公理を満たすものとする．

より一般的な定理（提示）

上で提示した定理 1.1 を証明する前に，加法を定義するときのために，より一般的な定理を示す．それは，N' の代わりにもっと一般的な（空でない）集合 X への写像を考えたものである．これを，示すべき定理として明示しておく．ここで，X を空でない集合，x_0 を X の元，$\varphi : X \to X$ を写像とする．

【定理 1.2】

次の条件を満たす写像 $f : N \to X$ がただ 1 つ存在する．

$$\text{(i)} \quad f(0) = x_0$$
$$\text{(ii)} \quad f \circ \sigma = \varphi \circ f$$

ここで，X, x_0, φ について，$X \neq \emptyset$ であること以外条件がないことに注意してほしい．

より一般的な定理（準備）

定理 1.2 を証明するためにいくつか準備をしておく．$N \times X$ の部分集合 A を，次の条件を満たす集合とする．

$$\text{(a)} \quad (0, x_0) \in A$$
$$\text{(b)} \quad (n, x) \in A \Longrightarrow (\sigma(n), \varphi(x)) \in A$$

このような集合 A 全体の集合族を $\mathscr{A}$ とする．また，集合 B を次のように定義する．

$$B = \bigcap_{A \in \mathscr{A}} A$$

【補題 1.3】

B は $\mathscr{A}$ の元の中で，集合の包含関係について最小である．

【証明】

$B \in \mathscr{A}$ さえ示せれば，B が包含関係について最小であることは定義より明らかである．よって，$B \in \mathscr{A}$ を示す．

$\forall A \in \mathscr{A}, (0, x_0) \in A$ なので $(0, x_0) \in B$ である．

$$\begin{aligned}(n, x) \in B &\Longrightarrow \forall A \in \mathscr{A}, (n, x) \in A \\ &\Longrightarrow \forall A \in \mathscr{A}, (\sigma(n), \varphi(x)) \in A \\ &\Longrightarrow (\sigma(n), \varphi(x)) \in B\end{aligned}$$

よって，B は条件 (a),(b) を満たすので $B \in \mathscr{A}$ である．

□

ここで任意の $n \in N$ に対して X の部分集合 X_n を次で定義する．

$$X_n = \{x \in X \mid (n, x) \in B\}$$

【補題 1.4】

すべての $n \in N$ に対して X_n は単項集合である．

【証明】

X_n が単項集合となるような $n \in N$ 全体の集合を S とおく．$S = N$ となることを示せばよい．$S \subset N$ であることはわかるので，Peano の公理 (N2) を用いて示す．

＜$0 \in S$ であること＞

$B \in \mathscr{A}$ より $(0, x_0) \in B$ なので，$x_0 \in X_0$ である．ここで，x_0 と相異なる $y \in X$ があり，$y \in X_0$ であると仮定する．このとき，$B' = B \setminus \{(0, y)\}$ とすると，$(0, y) \in B$ ($\because y \in X_0$) より，B' は B の真部分集合である．また，$(0, x_0) \neq (0, y)$ ($\because x_0 \neq y$) なので，$(0, x_0) \in B'$ となる．

さらに，$(n, x) \in B'$ とすると，Peano の公理 (N1) より $(\sigma(n), \varphi(x)) \neq (0, y)$ なので，$(\sigma(n), \varphi(x)) \in B'$ である．つまり，B' は条件 (a),(b) を満たすため，$B' \in \mathscr{A}$ となる．しかし，これは B の最小性（補題 1.3）に矛盾する．よって，X_0 は単項集合となり，$0 \in S$ である．

＜$\sigma(S) \subset S$ であること＞

これを示すには，$\forall k \in S, \sigma(k) \in S$ が示せればよい．$k \in S$ とし，$X_k = \{x_k\}$ とおく．このとき，$(k, x_k) \in B$ となるので $(\sigma(k), \varphi(x_k)) \in B$ である．よって，$\varphi(x_k) \in X_{\sigma(k)}$ となる．ここで，$\varphi(x_k)$ と相異なる $y \in X$ があり，$y \in X_{\sigma(k)}$ であると仮定する．このとき，$B' = B \setminus \{(\sigma(k), y)\}$ とすると，$(\sigma(k), y) \in B$ より，B' は B の真部分集合である．また，$(0, x_0) \neq (\sigma(k), y)$ ($\because$ Peano の公理 (N1)) なので，$(0, x_0) \in B'$ となる．

さらに，$(n, x) \in B'$ とする．$(\sigma(n), \varphi(x)) = (\sigma(k), y)$ と仮定すると，$\sigma(n) = \sigma(k)$ となり，これと σ の単射性より，$n = k$ となる．よって，$(n, x) = (k, x_k)$ となり，$\varphi(x) = \varphi(x_k)$ ($\because x = x_k$) となる．しかしこれは $\varphi(x) = y, \varphi(x_k) \neq y$ から明らかに矛盾する．したがって，$(\sigma(n), \varphi(x)) \neq (\sigma(k), y)$ でなければならない．ゆえに，$(\sigma(n), \varphi(x)) \in B'$ となり，B' は条件 (a),(b) を満たすため，$B' \in \mathscr{A}$ となる．しかし，これは B の最小性（補題 1.3）に矛盾する．よって，$X_{\sigma(k)}$ は単項集合となり，$\sigma(k) \in S$ である．

以上より，$0 \in S$ かつ$\sigma(S) \subset S$ が示されたので，Peano の公理 (N2) より $S = N$ である．

□

このことから，すべての $n \in N$ に対して X_n は単項集合であるので $X_n = \{x_n\}$ とする．証明中から，$x_{\sigma(n)} = \varphi(x_n)$ であることが分かる．これでようやく定理 1.2 が証明できる．

より一般的な定理（証明）

【定理 1.2（再提示）】

次の条件を満たす写像 $f : N \to X$ がただ 1 つ存在する．

(i) $f(0) = x_0$

(ii) $f \circ \sigma = \varphi \circ f$

【証明】

＜写像 f の存在性＞

$f : N \to X; n \mapsto x_n$ とする．まず，$f(0) = x_0$ であることは明らかである．次に，$f(\sigma(n)) = x_{\sigma(n)} = \varphi(x_n) = \varphi(f(n))$ とできるので，$f \circ \sigma = \varphi \circ f$ である．よって，条件 (i),(ii) を満たす写像 f が構成できた．

＜写像 f の一意性＞

条件 (i),(ii) を満たす 2 つの写像 f, f' を任意にとる．$\forall n \in N, f(n) = f'(n)$ を示せばよい．$S = \{n \in N \mid f(n) = f'(n)\}$ とおき，$S = N$ を示す．f, f' は条件 (i) を満たしているので，$f(0) = x_0 = f'(0)$ となる．よって，$0 \in S$ である．また，$n \in S$ とすると，条件 (ii) より

$$f(\sigma(n)) = \varphi(f(n)) = \varphi(f'(n)) = f'(\sigma(n))$$

とできるので，$\sigma(n) \in S$ である．よって，$\sigma(S) \subset S$ となり，$S = N$ である．

□

ここで，X, x_0, φ の代わりに $N, 0, \sigma$ を当てはめると，条件 (i),(ii) を満たす写像 $f : N \to N$ は N の恒等写像のみとなることが分かる．

定理 1.1 の証明

ここで定理 1.1 の証明を行う．

【定理 1.1（再提示）】

集合 N' と，元 $n' \in N'$，単射 $\sigma' : N' \to N'$ が Peano の公理を満たしているとする．このとき，次の条件を満たす全単射 $f : N \to N'$ がただ 1 つ存在する．

$$\text{(i)} \quad f(0) = 0'$$
$$\text{(ii)} \quad f \circ \sigma = \sigma' \circ f$$

【証明】

＜写像 f の存在性と一意性＞

定理 1.2 において，X, x_0, φ として $N', 0', \sigma'$ を当てはめると，条件 (i),(ii) を満たす写像 f がただ 1 つ構成できる．

＜写像 f の全単射性＞

写像 f が全単射であることを示すには，同値命題である f に逆写像が存在することを示せばよい．いま，集合 N と N' の役割を入れ替えることで，次の条件を満たす全単射 $f' : N' \to N$ がただ 1 つ得られる．

$$\text{(i)}' \quad f'(0') = 0$$
$$\text{(ii)}' \quad f' \circ \sigma' = \sigma \circ f'$$

写像 $g : N \to N$ を $g = f' \circ f$ と定義すると，$g(0) = f'(f(0)) = f'(0') = 0$ である．また，任意の $n \in N$ に対して

$$\begin{aligned} g(\sigma(n)) &= f'(f(\sigma(n))) \\ &= f'(\sigma'(f(n))) \\ &= \sigma(f'(f(n))) \\ &= \sigma(g(n)) \end{aligned}$$

とできるので，g は定理 1.2 の条件 (i),(ii) を満たす．定理 1.2 の一意性により，$g = f' \circ f$ は N の恒等写像である．同様にして，写像 $f \circ f'$ が N' の恒等写像となることが分かる．よって，f' は f の逆写像になっている．

□

1.1.4 自然数と“1”,“2”の定義

これまでの議論から，“Peano の公理を満たす集合”は本質的にただ 1 つしか存在しないことが分かった．よって，“Peano の公理を満たす集合”を $\mathbb{N}$ と書き，$\mathbb{N}$ の元を自然数ということにする．（単に集合 $\mathbb{N}$ を自然数ということもある．）また，$\sigma(0)$ を 1 と表し，$\sigma(\sigma(0)) = \sigma(1)$ を 2 と表すようにする．これでようやく“1”と“2”が定義できたので，“1”と“2”に関する議論ができる．しかし，まだ加法が定義できてないので，“$1+1$”が議論できない．なので次の節では自然数の加法を定義する．

1.2　自然数の加法

【命題 1.5】

任意の $n \in \mathbb{N}$ に対して，次を満たす写像 $\sigma_n : \mathbb{N} \to \mathbb{N}$ がただ 1 つ存在する．

$$\text{(i)}\ \ \sigma_n(0) = n$$
$$\text{(ii)}\ \ \sigma_n \circ \sigma = \sigma \circ \sigma_n$$

【証明】

定理 1.2 において，X, x_0, φ として $\mathbb{N}, n, \sigma$ を当てはめると，f として σ_n がただ 1 つ得られる．

□

ここで，$\mathbb{N}$ 上の演算 $\mathbb{N} \times \mathbb{N} \to \mathbb{N}; (m, n) \mapsto \sigma_n(m)$ を自然数の加法とし，$\sigma_n(m)$ を m, n の和といい，$m + n$ と表すようにする．

これで加法が定義できたので，本題である“$1 + 1 = 2$”について議論できるようになった．それぞれの定義から $1 + 1 = \sigma_1(1), 2 = \sigma(1)$ なので，$\sigma_1(1) = \sigma(1)$，特に $\sigma_1 = \sigma$ を示すのが最終的な目標となる．

これ以外にも，加法に関する様々な性質（交換法則，結合法則，簡約法則など）が証明できるが，今回の目的とは関係ないので，ここではしないことにする．

【定理 1.6】

$\sigma_1 = \sigma$ である．

【証明】

$\sigma(0) = 1, \sigma \circ \sigma = \sigma \circ \sigma$ は自明である．命題 1.5 の一意性により $\sigma_1 = \sigma$ である．

□

これで晴れて“$1 + 1 = 2$”が証明されたことになる．実は“$1 + 1 = 2$”の証明に直接関係があるのは定理 1.6 だけである．それまでの議論は，これを考察するための諸概念の定義に関する考察である．つまり，今回の証明の難しいところは，概念を定義すること自体であったり，定義できることを保証することだったのである．定理 1.1 を今回の議論において最も重要な定理と言ったように，定理 1.1 の証明，つまり自然数が定義できることを証明することが難解なのである．なので，それさえできてしまえば，それからは何ともあっけなく証明が終わってしまう．

1.3　第 1 章演習：自然数の性質

第 1 章で $1 + 1 = 2$ を証明してきた．しかし，自然数の持つ性質には全く触れてこなかった．ここでは，$1 + 1 = 2$ の証明のみを目的としていたため，それらについて触れずに議論できた．だが実際，自然数をこのように構成することで，自然数の諸性質が導かれることを見るのが面白く，本質的である．さらに第 2 章で整数を自然数から構成していくうえでも，自然数の性質を使うので，ここで一度性質を提示しておく．演習問題として，これらの性質が導かれることを証明してみるとよいだろう．

1.3.1　自然数の加法

まずは，自然数の加法についての性質である．次の数学的帰納法は加法についての性質とは言いにくいが，$n + 1$ が定義されていないと議論できないのでここで提示しておく．

【定理 1.7】（数学的帰納法 I）

任意の自然数 n について命題 $P(n)$ があり，次が成り立つとする．

(1) $P(0)$ は正しい

(2) $P(n)$ が正しいなら $P(n+1)$ も正しい

このとき，すべての自然数 n について $P(n)$ は正しい．
また，これを利用した証明の方法を数学的帰納法という．

これによって，自然数に関する証明がしやすくなる．（その威力は高校数学でも十分に理解できただろう．）次の加法に関する性質は，一部この数学的帰納法を用いるとやりやすいだろう．

【定理 1.8】＜加法に関する性質＞

$\forall m, n, k \in \mathbb{N}$ に対して，次が成り立つ．

(1) 単位元の存在：$n + 0 = 0 + n = n$

(2) 交換法則：$m + n = n + m$

(3) 結合法則：$(m + n) + k = m + (n + k)$

(4) 簡約法則：$m + k = n + k \Longrightarrow m = n$

1.3.2 自然数の順序関係

次に自然数の順序関係の性質を述べるが，まだ順序関係を定義していないのでここで定義する．

【定義】2 つの自然数 m, n に対して，関係 $\leq$ を次のように定義する．

$$m \leq n \Longleftrightarrow \exists k \in \mathbb{N} \text{ s.t. } n = m + k$$

$m \leq n$ を $n \geq m$ とも書く．
また，$m \leq n$ かつ $m \neq n$ のとき $m < n$ とする．

これではまだ，この関係 $\leq$ が順序関係であることはわからない．なので，それを証明する必要がある．具体的には，関係 $\leq$ が次の 3 つの条件を満たすことを示せばよい．

反射律 :$\forall n \in \mathbb{N}, n \leq n$

推移律 :$\forall m, n, k \in \mathbb{N}, m \leq n$ かつ $n \leq k \Longrightarrow m \leq k$

反対称律 :$\forall m, n \in \mathbb{N}, m \leq n$ かつ $n \leq m \Longrightarrow m = n$

【命題 1.9】

上の定義による自然数上の関係 $\leq$ は順序関係である．

ここで，2 つの自然数 m, n が $m < n$ となるとき，m は n より小さいといい，n は m より大きいという．

これで，自然数上の順序関係が定義できたので，それに関する性質を示そう．

【定理 1.10】＜順序関係に関する性質＞

(1) $\forall m, n \in \mathbb{N}$ について，

$$m < n \Longleftrightarrow \exists k \in \mathbb{N}, k \neq 0 \text{ s.t. } n = m + k$$

(2) 関係 $<$ は推移律を満たす．
(3) $\forall m, n, k \in \mathbb{N}$ に対して，

$$m < n \Longleftrightarrow m + k < n + k$$

(4) $\forall m, n \in \mathbb{N}$ について，

$$m < n \Longrightarrow m + 1 \leq n$$
$$m < n + 1 \Longrightarrow m \leq n$$

(5) $\forall m, n \in \mathbb{N}$ について，$m > n, m = n, m < n$ のいずれか 1 つのみが成り立つ．
(6) 整列性：$\mathbb{N}$ の任意の空でない部分集合は最小元を持つ．

この順序関係とその性質を用いることで，数学的帰納法の応用的なものが示される．

【定理 1.11】（数学的帰納法 II）

任意の自然数 n について命題 $P(n)$ があり，次が成り立つとする．

(1) $P(0)$ は正しい
(2) $\forall k \in \mathbb{N}, 0 \leq k \leq n$ について，
$P(k)$ が正しいなら $P(n+1)$ も正しい

このとき，すべての自然数 n について $P(n)$ は正しい．
また，これを利用した証明の方法も数学的帰納法という．

1.3.3 自然数の乗法

最後に自然数の乗法に関する性質を述べる．これも順序関係と同様，定義がなされていないので，定義から始める．まず，加法のときと同じように，次の命題を示す．

【命題 1.12】

任意の $n \in \mathbb{N}$ に対して，次を満たす写像 $\pi_n : \mathbb{N} \to \mathbb{N}$ がただ 1 つ存在する．

(i) $\pi_n(0) = 0$
(ii) $\pi_n \circ \sigma = \sigma_n \circ \pi_n$

これにより，自然数の乗法を定義する．

【定義】$\pi_n(m)$ を m, n の積といい，$m \times n$ または $m \cdot n$ と表すようにする．また，この演算を自然数の乗法という．

乗法の定義が済んだところで，それの性質を述べる．(4) の分配法則は乗法のみでなく，加法と乗法についての性質だが，ここではそれもひとまとまりにして書いておく．

【定理 1.13】＜乗法に関する性質＞

$\forall m, n, k \in \mathbb{N}$ に対して，次が成り立つ．

(1) 単位元の存在：$n \times 1 = 1 \times n = n$

(2) 交換法則：$m \times n = n \times m$

(3) 結合法則：$(m \times n) \times k = m \times (n \times k)$

(4) 分配法則：$m \times (n + k) = (m \times n) + (m \times k)$

$$(m + n) \times k = (m \times k) + (n \times k)$$

(5) 加法単位元との積：$n \times 0 = 0 \times n = 0$

(6) $m \neq 0$ かつ $n \neq 0 \Longrightarrow m \times n \neq 0$

(7) $k \neq 0$ のとき，$m < n \Longrightarrow m \times k < n \times k$

(8) 簡約法則：$k \neq 0$ のとき，$m \times k = n \times k \Longrightarrow m = n$

第2章　$(-1)\times(-1)$が1であることについて

前章で$1+1=2$の証明を行った．次はこれと同等かそれ以上の疑問であると思われる$(-1)\times(-1)=1$を証明していきたいと思う．-1は自然数ではなく，整数と呼ばれるものである．よって，前章で定義した自然数だけではこの数式を考えることができない．なので，今回は整数を自然数から構成するところからはじめ，整数上の演算を定義し，$(-1)\times(-1)=1$を証明していく．前章と違い，今回は自然数という土台がすでにあるところで考察をしていかなくてはいけない．なので，前章よりも確認すべき事項が増えるため，少々難しくなってしまうだろう．

2.1　自然数の復習

自然数全体の集合$\mathbb{N}$とはPeanoの公理を満たす集合である．自然数は加法に関して，単位的，結合的ではあるが，可逆的ではない．このような構造をモノイドという．あと可逆性さえ与えれば，これは群という構造をもつようになる．自然数を群となるように拡張したものが整数である．これにより，まず整数を構成していく．

2.2　自然数から整数へ

2.2.1　整数の定義

「自然数を群に拡張する」ことを目的として整数を構成していく．まず次のような関係$\sim$を考える．$\forall(a,b),(c,d)\in\mathbb{N}\times\mathbb{N}$について

$$(a,b)\sim(c,d)\Longleftrightarrow a+d=c+b$$

【命題 2.1】

上で定義した$\mathbb{N}\times\mathbb{N}$上の関係$\sim$は同値関係である．

【証明】

$a+b=a+b$は明らかなので$(a,b)\sim(a,b)$である．よって，関係$\sim$は反射律を満たす．

次に，$(a,b)\sim(c,d)$とすると，$a+d=c+b$なので$c+b=a+d$である．よって，$(c,d)\sim(a,b)$となる．ゆえに，対称律も満たす．

また，$(a,b)\sim(c,d),(c,d)\sim(e,f)$とすると，$a+d=c+b$と$c+f=e+d$が成り立つ．両辺を足して，$a+d+c+f=c+b+e+d$となる．自然数の加法の可換性，簡約性を利用すると，$a+f=e+b$である．よって，$(a,b)\sim(e,f)$が成り立ち，推移律も満たす．

□

よって，$\mathbb{N}\times\mathbb{N}$の$\sim$による類別ができ，その同値類の集合を$\mathbb{Z}$とする．

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

また，$(m,n) \in \mathbb{N} \times \mathbb{N}$ を代表元とする同値類を $[m,n]$ とする．つまり，

$$\mathbb{Z} = \{[m,n] \mid m,n \in \mathbb{N}\}$$

この $\mathbb{Z}$ を整数全体の集合といい，$\mathbb{Z}$ の元を整数という．

$a,b,c,d \in \mathbb{N}$ について，次が成り立つ．

$$[a,b] = [c,d] \Longleftrightarrow (a,b) \sim (c,d) \Longleftrightarrow a+d = c+b$$

【補題 2.2】

(1) $\forall m,n \in \mathbb{N}, [m,m] = [n,n]$

(2) $\forall m,n,k \in \mathbb{N}, [m+k, n+k] = [m,n]$

【証明】

(1)

任意に自然数 m,n をとる．自然数の加法が可換であることから，

$$m+n = n+m$$

である．よって，$[m,m] = [n,n]$ となる．

(2)

任意の自然数 m,n,k をとる．自然数の加法について，可換であり，結合法則が成り立つことから，

$$(m+k)+n = m+(n+k)$$

となる．よって，$[m+k, n+k] = [m,n]$ である．

□

2.2.2 整数の加法と群

整数の加法を次のように定義する．

【整数の加法】

$\forall [a,b],[c,d] \in \mathbb{Z}$ に対して

$$[a,b] + [c,d] = [a+c, b+d]$$

$$\begin{aligned}
&[a,b] = [a',b'], [c,d] = [c',d'] \\
&\Longrightarrow a+b' = a'+b, c+d' = c'+d \\
&\Longrightarrow (a+b')+(c+d') = (a'+b)+(c'+d) \\
&\Longrightarrow (a+c)+(b'+d') = (a'+c')+(b+d) \\
&\Longrightarrow [a+c, b+d] = [a'+c', b'+d']
\end{aligned}$$

よって，上の定義による整数の加法は well-defined である．

これで整数とその加法が定義できたが，もともとの動機であった「自然数を群に拡張する」ことは本当にできているのだろうか．実際，整数がこの加法で群になることがわかる．

【定理 2.3】

整数全体の集合 $\mathbb{Z}$ は加法について群である．さらに，可換であり，簡約的でもある．

【証明】

＜結合法則＞

任意に整数 $[a,b],[c,d],[e,f]$ をとる．自然数は加法について結合的なので，

$$\begin{aligned}&([a,b]+[c,d])+[e,f]\\&\quad=[(a+c)+e,(b+c)+f]\\&\quad=[a+(c+e),b+(d+f)]\\&\quad=[a,b]+([c,d]+[e,f])\end{aligned}$$

となり，結合法則が成り立つ．

＜単位元の存在＞

補題 2.2(2) と自然数の加法が可換であることから，任意の自然数 n について $[n,n]$ と表される元が，整数の加法における単位元であることがわかる．また，(1) からそれが一意であることもわかる．

＜逆元の存在＞

自然数の加法の可換性と補題 2.2(1) から，任意の整数 $[a,b]$ に対して $[b,a]$ が逆元となっていることがわかる．

＜可換性＞

任意に整数 $[a,b],[c,d]$ をとる．このとき，自然数の加法の可換性より，

$$\begin{aligned}[a,b]+[c,d]&=[a+c,b+d]\\&=[c+a,d+b]\\&=[c,d]+[a,b]\end{aligned}$$

となるので，可換である．

＜簡約法則＞

任意に整数 $[a,b],[c,d],[e,f]$ をとる．自然数の加法における可換性，結合性，簡約性を用いると，

$$\begin{aligned}&[a,b]+[e,f]=[c,d]+[e,f]\\&\quad\Longrightarrow[a+e,b+f]=[c+e,d+f]\\&\quad\Longrightarrow(a+e)+(d+f)=(c+e)+(b+f)\\&\quad\Longrightarrow(a+d)+(e+f)=(c+b)+(e+f)\\&\quad\Longrightarrow a+d=c+b\\&\quad\Longrightarrow[a,b]=[c,d]\end{aligned}$$

となるので，簡約法則が成り立つ．

□

よって，整数は自然数から群に拡張されたものであることがわかった．さらに，自然数で成り立っていた諸性質（可換性や簡約性など）もしっかりと受け継がれている．

整数 $[a,b]$ の逆元 $[b,a]$ を $-[a,b]$ と表すことにする．また，整数 m,n に対して $m+(-n)$ を $m-n$ と省略して表記することにする．この表記により,「逆元を右から足す」という新たな二項演算 $-$ が見える．これを減法という．

2.2.3　整数の乗法

ここで，本題の $(-1)\times(-1)=1$ を考察するために，整数についての乗法を定義する．

【整数の乗法】
$\forall[m,n],[k,l]\in\mathbb{Z}$ に対して

$$[m,n]\times[k,l]=[m\cdot k+n\cdot l,m\cdot l+n\cdot k]$$

（$[m,n]\times[k,l]$ は $[m,n]\cdot[k,l]$ とも書く．）

$$\begin{aligned}
&[m,n]=[m',n'],[k,l]=[k',l']\\
&\Longrightarrow m+n'=m'+n,k+l'=k'+l\\
&\Longrightarrow(m+n')\cdot k+(m'+n)\cdot l+m'\cdot(k+l')+n'\cdot(k'+l)\\
&\qquad=(m'+n)\cdot k+(m+n')\cdot l+m'\cdot(k'+l)+n'\cdot(k+l')\\
&\Longrightarrow(m\cdot k+n\cdot l)+(m'\cdot l'+n'\cdot k')=(m'\cdot k'+n'\cdot l')+(m\cdot l+n\cdot k)\\
&\Longrightarrow[m\cdot k+n\cdot l,m\cdot l+n\cdot k]=[m'\cdot k'+n'\cdot l',m'\cdot l'+n'\cdot k']
\end{aligned}$$

よって，上の定義による整数の乗法は well-defined である．

2.2.4　自然数と整数

これで整数と演算が定義できたのだが，このままでは，自然数と整数は全くの別ものである．つまり，普段我々が使っているような自然数を包含するような集合としての整数ではないのである．そのために，自然数を整数の一部と見ても問題がないことを確かめる．まず，次のような自然数から整数への写像 φ を考える．

$$\begin{array}{rccc}
\varphi: & \mathbb{N} & \longrightarrow & \mathbb{Z}\\
& \cup & & \cup\\
& n & \longmapsto & [n,0]
\end{array}$$

$\forall m,n\in\mathbb{N},\varphi(m+n)=\varphi(m)+\varphi(n)$ は明らかなので，φ はモノイドの準同型である．また，$\forall m,n\in\mathbb{N}$ に対して

$$\begin{aligned}
m\neq n&\Longrightarrow m+0\neq n+0\\
&\Longrightarrow[m,0]\neq[n,0]
\end{aligned}$$

なので，φ は単射準同型である．よって，$n\in\mathbb{N}$ に対して，$n=[n,0]$ とすることで，$\mathbb{N}$ を $\mathbb{Z}$ の部分集合とみることができる．

また，$[m,n]\in\mathbb{Z}$ の逆元が $[n,m]$ であることから，整数としての元 $n=[n,0]$ の逆元 $-n$ は $[0,n]$ である．さらに，$[m,n]=[m,0]+[0,n]=m-n$ とできるので，

$$\mathbb{Z}=\{m-n\mid m,n\in\mathbb{N}\}$$

となる．

【定理 2.4】

$\forall a \in \mathbb{Z}$ に対して，次の 3 つのどれか 1 つのみが成り立つ．

(1) $\exists k \in \mathbb{N}, k \neq 0$ s.t. $a = -k$

(2) $a = 0$

(3) $\exists l \in \mathbb{N}, l \neq 0$ s.t. $a = l$

【証明】

＜どれか 1 つしか成立しないこと＞

(1) と (2)，(2) と (3) が同時に成り立たないことは明らかである．(1) と (3) が同時に成り立ったとすると，$a = -k = l$ となるので，$[0, k] = [l, 0]$ となる．よって，$0 + 0 = k + l$ であるので，$k = l = 0$ となる．つまり，$a = 0$，(2) も成り立つことになり，先の考察に矛盾する．

＜どれか 1 つは成立すること＞

$m, n \in \mathbb{N}$ を用いて，$a = m - n$ とする．任意の 2 つの自然数 m, n について，$m > n, m = n, m < n$ のいずれか 1 つのみが成り立つことを用いる．

$m > n$ のとき，$\exists k \in \mathbb{N}, k \neq 0$ s.t. $m = n + k$ より

$$a = [m, n] = [m, m + k] = [0, k] = -k$$

$m = n$ のとき

$$a = [m, n] = [m, m] = [0, 0] = 0$$

$m > n$ のとき，$\exists l \in \mathbb{N}, l \neq 0$ s.t. $n = m + l$ より

$$a = [m, n] = [n + l, n] = [l, 0] = l$$

よって，(1) から (3) のいずれかが成り立つ．

□

$-\mathbb{N} = \{-n \mid n \in \mathbb{N}\}$ とすると，定理 2.4 より次のことがわかる．

$$\mathbb{Z} = \mathbb{N} \cup -\mathbb{N}$$
$$\mathbb{N} \cap -\mathbb{N} = \{0\}$$

特に，1 つ目の式より

$$\mathbb{Z} = \{n \text{ or } -n \mid n \in \mathbb{N}\}$$

と表せることが分かる．

2.3 $(-1) \times (-1) = 1$ について

これで，本題の $(-1) \times (-1) = 1$ についての考察をする準備が完了した．もとの定義から整数 $1, -1$ は $[1, 0], [0, 1]$ であることに注意すれば，

$$\begin{aligned}(-1) \times (-1) &= [0, 1] \times [0, 1] \\ &= [0 \cdot 0 + 1 \cdot 1, 0 \cdot 1 + 1 \cdot 0] \\ &= [1, 0] \\ &= 1\end{aligned}$$

となるので，$(-1)\times(-1)=1$ が示せた．また，整数 $[m,n]$ について，

$$\begin{aligned}(-1)\times[m,n] &= [0,1]\times[m,n]\\ &= [0\cdot m+1\cdot n, 0\cdot n+1\cdot m]\\ &= [n,m]\\ &= -[m,n]\end{aligned}$$

なので，これと整数の乗法の可換性，結合性より，$\mathbb{N}\setminus\{0\}$ の元を正の整数，$-\mathbb{N}\setminus\{0\}$ の元を負の整数ということにすると，

$$(\text{負の整数})\times(\text{負の整数})=(\text{正の整数})$$

という，より一般的なこともわかる．

2.4 第 2 章演習：整数の性質

第 2 章で整数について定義からして，$(-1)\times(-1)=1$ を証明してきた．しかし，第 1 章と同様，整数が持つ性質については，一部を除いて触れずにいた．だが，第 1 章演習でも述べた通り，これらの議論の本質的な部分は，整数をこのように構成することで，整数の諸性質が導くことができるというところにある．よって，それらについて，ここに明記するので証明いてみるとよい．

加法についての性質は，第 2 章で扱ったので省略する．なお，そのときの議論から，整数は自然数を性質を保ったまま，モノイドから群に拡張したものだということが分かった．しかし，保たれていることを示したのは，加法についての性質だけであり，本当に自然数の性質を保っていることを見るには，自然数の順序関係と乗法についての性質も保たれていることを証明する必要がある．

2.4.1 整数の順序関係

自然数同様，整数の順序関係には触れていないので，定義から始める．

【定義】2 つの整数 m,n に対して，関係 $\leq$ を次のように定義する．

$$m\leq n \Longleftrightarrow \exists k\in\mathbb{N}\ \text{s.t.}\ n=m+k$$

$m\leq n$ を $n\geq m$ とも書く．
また，$m\leq n$ かつ $m\neq n$ のとき $m<n$ とする．

自然数のときと，何も変わらないように見えるが，任意の整数は 2 つの自然数 m,n を用いて $[m,n]$ と表されるものだったことに注意する必要がある．この関係も，自然数の順序関係と同様に順序関係であることが示される．

【命題 2.5】

上の定義による整数上の関係 $\leq$ は順序関係である．

自然数と同様に，2 つの整数 m,n が $m<n$ となるとき，m は n より小さいといい，n は m より大きいという．

整数でも順序関係が定義できたので，順序関係に関する次の性質を証明しよう．

【定理 2.6】＜順序関係に関する性質 I ＞

(1) $\forall m, n \in \mathbb{Z}$ について，

$$m < n \Longleftrightarrow \exists k \in \mathbb{Z}, k \neq 0 \text{ s.t. } n = m + k$$

(2) 関係 $<$ は推移律を満たす．

(3) $\forall m, n, k \in \mathbb{Z}$ に対して，

$$m < n \Longleftrightarrow m + k < n + k$$

(4) $\forall m, n \in \mathbb{Z}$ について，

$$m < n \Longrightarrow m + 1 \leq n$$
$$m < n + 1 \Longrightarrow m \leq n$$

(5) $\forall m, n \in \mathbb{Z}$ について，$m > n, m = n, m < n$ のいずれか 1 つのみが成り立つ．

これらから，整数は自然数の順序関係についての性質のうち，整列性以外は保存されていることが分かる．整数に整列性はないが，その代わり次の定理を満たす．

【定理 2.7】

S を空でない $\mathbb{Z}$ の部分集合とする．

(1) $\exists m \in \mathbb{Z}$ s.t. $\forall n \in S, n < m$ となるとき，S は最大元を持つ．

(2) $\exists m \in \mathbb{Z}$ s.t. $\forall n \in S, n > m$ となるとき，S は最小元を持つ．

さらに，整数には加法についての逆元があるので，それについても考えることができる．

【定理 2.8】＜順序関係に関する性質 II ＞

$\forall m, n \in \mathbb{Z}$ に対して，次が成り立つ．

$$m < n \Longleftrightarrow -m > -n$$

また，定理 2.6(5) で $n = 0$ とすることで，任意の整数 m について，$m > 0, m = 0, m < 0$ のいずれか 1 つのみが成り立つことが分かる．さらに，次のこともわかる．

【定理 2.9】

$\forall n \in \mathbb{Z}$ に対して，次が成り立つ．

$$(1)\ \ n > 0 \Longleftrightarrow n \in \mathbb{N} \setminus \{0\}$$
$$(2)\ \ n < 0 \Longleftrightarrow n \in -\mathbb{N} \setminus \{0\}$$

これで，2.4 節で暗に $\mathbb{N} \setminus \{0\}$ の元を正の整数，$-\mathbb{N} \setminus \{0\}$ の元を負の整数ということにしたことが，正当化される．もちろん，“ 正 ”というものを“ 0 より大きいもの ”と，我々が普段使っている意味でとらえたときの話ではあるが．ここで，正と負について明確に述べておく．$n \in \mathbb{Z}$ が $n > 0$ となるとき n は正であるといい，$n < 0$ となるとき n は負であるという．

2.4.2 整数の乗法

最後に，整数の乗法の性質について示そう．整数の乗法はすでに定義してあるので，定義は省略する．

【定理 2.10】＜乗法に関する性質 I＞

$\forall m, n, k \in \mathbb{Z}$ に対して，次が成り立つ．

(1) 単位元の存在：$n \times 1 = 1 \times n = n$

(2) 交換法則：$m \times n = n \times m$

(3) 結合法則：$(m \times n) \times k = m \times (n \times k)$

(4) 分配法則：$m \times (n + k) = (m \times n) + (m \times k)$

$(m + n) \times k = (m \times k) + (n \times k)$

(5) 加法単位元との積：$n \times 0 = 0 \times n = 0$

(6) $m \neq 0$ かつ $n \neq 0 \Longrightarrow m \times n \neq 0$

(7) 簡約法則：$k \neq 0$ のとき，$m \times k = n \times k \Longrightarrow m = n$

よって，整数は自然数の乗法の性質を受け継いでいることが分かった．これまでのことから，整数は自然数を，性質を保ったまま拡張したものだということが理解できる．

さらに，ここで整数は乗法についてモノイドになっていることが分かる．加法について可換な群で，乗法についてモノイドになっていて、分配法則が成り立つものを環という．なので，整数は群であるだけでなく，環でもあることが分かる．

順序関係のときと同様に，逆元についての性質も書いておく．

【定理 2.11】＜乗法に関する性質 II＞

$\forall m, n, k \in \mathbb{Z}$ に対して，次が成り立つ．

(1) $(-m) \times n = m \times (-n) = -(m \times n)$

(2) $(-m) \times (-n) = m \times n$

(3) $m \times (n - k) = (m \times n) - (m \times k)$

(4) $(m - n) \times k = (m \times k) - (n \times k)$

乗法と順序関係についても述べておく．

【定理 2.12】

$\forall m, n, k \in \mathbb{Z}$ に対して，次が成り立つ．

(1) $k > 0$ ならば，$m < n \Longleftrightarrow mk < nk$

(2) $k < 0$ ならば，$m < n \Longleftrightarrow mk > nk$

(3) $m > 0$ ならば，$n > 0 \Longleftrightarrow mn > 0$

$n < 0 \Longleftrightarrow mn < 0$

(4) $m < 0$ ならば，$n > 0 \Longleftrightarrow mn < 0$

$n < 0 \Longleftrightarrow mn > 0$

第3章　おまけ：整数論の基礎

第 2 章で整数を定義した．そして，第 2 章演習も通して整数の性質について述べてきた．しかし，それは整数の持つ性質のごく一部に過ぎない．整数論という研究分野が存在するほど，整数には多くの性質があり，すべては紹介できないほどにもなる．その中でも今回，高校までにも学んできたような，整数に関する基礎的な性質，特に，約数や倍数，素数や素因数分解といったものを紹介しようと思う．以降，整数の乗法について，演算子 $\times$ または $\cdot$ は（わかりにくい場合を除き）省略して書くことにする．つまり，$m \times n$ や $m \cdot n$ を単に mn と書く．

3.1　整数の絶対値

まず，整数の絶対値について紹介する．

【整数の絶対値】
任意の整数 n について，n の絶対値 $|n|$ を次で定義する．

$$|n| = \begin{cases} n & n > 0 \\ 0 & n = 0 \\ -n & n < 0 \end{cases}$$

この絶対値について次の簡単な命題たちが示される．

【命題 3.1】
任意の整数 m, n, k について，次が成り立つ．

(1) $|n| \geq 0$
(2) $|n| = 0 \Longleftrightarrow n = 0$
(3) $n \leq |n|$
(4) $|-n| = |n|$
(5) $|mn| = |m||n|$
(6) $|m+n| \leq |m| + |n|$
(7) $|m-n| \leq |m| + |n|$
(8) $|m| - |n| \leq |m+n|$
(9) $|m| - |n| \leq |m-n|$

この命題の証明は省かせてもらう．気になる人は自分で証明してみるとよいだろう．

(6) の不等式は三角不等式と呼ばれる．また，これらと整数の性質の一部から，この絶対値は整数上の距離を引き起こすことがわかる．具体的には，2 つの整数 m, n に対して，それらの差の絶対値 $|m-n|$ を考えると，これは整数上の距離関数になっている．

3.2　整数の整除

ここまでに整数に加法，減法，乗法を定義してきた．小学校の頃からおなじみの四則演算は，これら 3 つの演算と除法を合わせて言うものである．しかし，周知のとおり整数の割り算は必ずしも整数になるとは限らない．つまり，整数上には除法は定義できない．しかし，これまた小学生のときに学んだ，余りという概念を使えば，整数上でも除法のようなものが考えられる．それは，ときに余り付き割り算などと呼ばれることもある．この節では，この余り付き割り算について紹介する．特に，余りが 0 のとき，つまり割り切れるときに焦点を当てて話す．

以降，正の整数全体の集合 $(\{n \in \mathbb{Z} \mid n > 0\} = \mathbb{N} \setminus \{0\})$ を $\mathbb{Z}^+$ と書くことにする．

【定理 3.2】

$a \in \mathbb{Z}, b \in \mathbb{Z}^+$ とする．このとき，

$$a = bq + r \qquad (0 \leq r < b)$$

となる $q, r \in \mathbb{Z}$ がただ 1 組存在する．
またこのとき，q, r をそれぞれ a を b で割った商，剰余（余り）という．

【証明】

まず，q, r の存在性を示す．

$$r = \min\{n \in \mathbb{N} \mid \exists q \text{ s.t. } a = bq + n\}$$

とおく．$\mathbb{N}$ の整列性により，このような r の存在が保証される．いま，ある整数 q が存在して，

$$a = bq + r$$

が成り立っているとする．もし仮に $b \leq r$ なら，

$$0 \leq r - b < r \ , \ a = b(q-1) + (r-b)$$

となり，r の最小性に矛盾する．よって，$0 \leq r < b$ である．

次に一意性を示す．

$$a = bq + r \qquad (0 \leq r < b)$$
$$a = bq' + r' \quad (0 \leq r' < b)$$

とすると，

$$b(q - q') = r' - r$$

$q \neq q'$ と仮定すると，

$$b \leq b|q - q'| = |r' - r| \leq \max\{r, r'\} < b$$

これは矛盾である．よって，$q = q', r = r'$ でないといけない．

□

$a, b \in \mathbb{Z}$ に対して，$q \in \mathbb{Z}$ があり，

$$a = bq$$

となるとき，a は b で割り切れるという．これを記号で

$$b \mid a$$

と書く．また，このとき a を b の倍数といい，b を a の約数という．

【定理 3.3】

$\forall a, b \in \mathbb{Z}$ に対し，次が成り立つ．

$$\begin{aligned} a \mid b &\iff -a \mid b \\ &\iff a \mid -b \end{aligned}$$

【証明】

任意に整数 a, b をとる．このとき，

$$\begin{aligned} a \mid b &\iff \exists q \in \mathbb{Z} \text{ s.t. } b = aq \\ &\iff \exists q' \in \mathbb{Z} \text{ s.t. } b = a \cdot (-q') \qquad (\because q = -q') \\ &\iff \exists q' \in \mathbb{Z} \text{ s.t. } b = (-a)q' \\ &\iff -a \mid b \end{aligned}$$

また，

$$\begin{aligned} a \mid b &\iff \exists q \in \mathbb{Z} \text{ s.t. } b = aq \\ &\iff \exists q' \in \mathbb{Z} \text{ s.t. } b = a \cdot (-q') \\ &\iff \exists q' \in \mathbb{Z} \text{ s.t. } b = -(aq') \\ &\iff \exists q' \in \mathbb{Z} \text{ s.t. } -b = aq' \\ &\iff a \mid -b \end{aligned}$$

よって題意は満たされた．

□

【定理 3.4】

$\forall a, b, c \in \mathbb{Z}$ に対し，次が成り立つ．

(1) $a \mid b \Longrightarrow a \mid bc$

(2) $c \neq 0$ のとき，$a \mid b \iff ac \mid bc$

(3) $a \mid b$ かつ $a \mid c \Longrightarrow a \mid b + c$

【証明】

(1)

$a \mid b$ とすると，整数 q が存在して，$b = aq$ となる．よって，$bc = aqc$ となり，$qc \in \mathbb{Z}$ なので，$a \mid bc$ である．

(2)

$c \neq 0$ とし，$a \mid b$ であるとする．いま，整数 q が存在して，$b = aq$ となっている．両辺に c をかけて，$bc = aqc = (ac)q$ となり，$ac \mid bc$ である．

逆に，$ac \mid bc$ とすると，整数 q' が存在して，$bc = acq'$ となる．これより，$bc - acq' = c(b - aq') = 0$ が得られる．$c \neq 0$ なので，$b - aq' = 0$ であり，$b = aq'$ となる．よって，$a \mid b$ である．

(3)

$a \mid b$ かつ $a \mid c$ とすると，ある整数 q, q' があり，$b = aq, c = aq'$ となっている．よって，$b + c = aq + aq' = a(q + q')$ となり，$q + q' \in \mathbb{Z}$ より $a \mid b + c$ である．

□

以下 2 つの定理は正の整数についての話であることに注意してほしい．つまり，以下の定理は負の整数への拡張ができない．$-1 \mid 1, 1 \mid -1$ であることを考えれば，理由は明らかだろう．

【定理 3.5】

$\forall a, b \in \mathbb{Z}^+$ に対して，$a \mid b$ ならば $a \leq b$ である．

【証明】

$a, b \in \mathbb{Z}^+$ を任意にとり，$a \mid b$ とする．ある整数 q が存在して，$b = aq$ となる．ここで，$q \leq 0$ と仮定すると，$a > 0, q \leq 0$ より $b = aq \leq 0$ となり，$b \in \mathbb{Z}^+$ に矛盾．よって，$q > 0$ つまり $q \geq 1$ でなければならない．したがって，

$$b = aq \geq a \cdot 1 = a$$

□

【定理 3.6】

$\forall a, b, c \in \mathbb{Z}^+$ に対し，次が成り立つ．

(1) $a \mid a$

(2) $a \mid b$ かつ $b \mid a \Longrightarrow a = b$

(3) $a \mid b$ かつ $b \mid c \Longrightarrow a \mid c$

【証明】

(1)

$\forall a \in \mathbb{Z}^+$ について，$a = a \cdot 1$ より明らか．

(2)

$a \mid b$ かつ $b \mid a$ とすると，$a \leq b$ かつ $b \leq a$ である．そうなるのは，$a = b$ のときのみである．

(3)

$a \mid b$ かつ $b \mid c$ とすると，ある整数 q, q' が存在して，$b = aq, c = bq'$ となっている．よって，$c = aqq'$ となり，$a \mid c$ である．

□

3.3 公約数と公倍数

整数について，余り付き割り算を導入して，余りが 0，つまり割り切れるときについて紹介した．約数や倍数からは，最大公約数や最小公倍数といったとても重要なものが考えられる．これは整数論においても重要な概念であり，高校数学でも扱われる．次はそれらについて紹介しようと思う．

整数 a, b に対し，a と b のどちらも割り切る整数を a と b の公約数という．つまり，

$$d \text{ は } a \text{ と } b \text{ の公約数} \Longleftrightarrow d \mid a \text{ かつ } d \mid b$$

ここで，a と b の公約数全体の集合を D とおくと，$\forall d \in D$ に対し，$d \mid |a|$ かつ $d \mid |b|$ であるので，$d \leq |a|$ かつ $d \leq |b|$ となる．よって，整数の性質（定理 2.7）から，D は最大元を持つことが分かる．このような，a と b の公約数のうち最大のものを a と b の最大公約数といい，$\gcd(a, b)$ と書く．これは 3 つ以上（有限個）の整数の組 $a_1, a_2, \ldots, a_n$ でも考えることができ，$a_1, a_2, \ldots, a_n$ の公約数のうち最大のものを $a_1, a_2, \ldots, a_n$ の最大公約数といい，$\gcd(a_1, a_2, \ldots, a_n)$ と書くことにする．

また，整数 a, b に対し，a と b の両方の倍数である整数を a と b の公倍数という．つまり，

$$m \text{ は } a \text{ と } b \text{ の公倍数} \iff a \mid m \text{ かつ } b \mid m$$

a と b の正の公倍数全体の集合を M^+ とおくと，$\forall m \in M^+$ に対して，$0 < m$ なので，M^+ には最小元がある．そのような a と b の正の公倍数のうち最小のものを a と b の最小公倍数といい，$\mathrm{lcm}(a, b)$ と書く．3 つ以上の組の場合も最大公約数と同じように表記する．

【定理 3.7】

$\forall a, b, m, d \in \mathbb{Z}$ に対し，次が成り立つ．

$$m : a \text{ と } b \text{ の公倍数} \iff \mathrm{lcm}(a, b) \mid m$$
$$d : a \text{ と } b \text{ の公約数} \iff d \mid \gcd(a, b)$$

【証明】

＜上段＞

$\mathrm{lcm}(a, b) = l$ とおき，m を a と b の公倍数とする．

$$m = lq + r \qquad (0 \leq r < l)$$

となる整数 q, r が存在する．このとき，

$$r = m - lq$$

であり，m, l が a と b の公倍数であることから，$m - lq = r$ も a と b の公倍数である．l が正の公倍数のうち最小のものだったので，$r < l$ である公倍数 r は正の公倍数ではない．これと $0 \leq r$ より，$r = 0$ である．よって，$m = lq$ となり，$l \mid m$ である．

＜下段＞

$\gcd(a, b) = g$ とおき，d を a と b の公約数とする．また，$\mathrm{lcm}(g, d) = l'$ とする．いま，仮定から a, b はどちらも g, d 両方の倍数になっているので，a, b は g と d の公倍数である．よって，a, b は l' の倍数となる（上段）．つまり，l' は a と b の公約数である．ここで，l' の取り方から $g \leq l'$ であるが，最大公約数 g の最大性から $g = l'$ となる．l' は d の倍数だったので，d は g の約数となる．

□

【定理 3.8】

$\forall a, b, c \in \mathbb{Z}$ に対し，次が成り立つ．

(1) $\gcd(a, b) = \gcd(b, a)$

(2) $\gcd(a, b, c) = \gcd(\gcd(a, b), c)$

【証明】

(1)

ある整数が a と b の公約数であることと，b と a の公約数であることは明らかに同値である．よって，それらの最大元である最大公約数は同じものである．

(2)

$\gcd(a, b, c) = g, \gcd(\gcd(a, b), c) = g', \gcd(a, b) = g''$ とおく．$g \mid a, g \mid b$ より，$g \mid g''$ となり，これと $g \mid c$ より，$g \mid g'$ である．また，$g' \mid g''$ より，$g' \mid a, g' \mid b$，これと $g' \mid c$ から，$g' \mid g$ となる．$g \mid g'$ と $g' \mid g$ より，$g = g'$ である．

□

【定理 3.9】

$\forall a, b, c \in \mathbb{Z}$ に対し，次が成り立つ．

(1) $\mathrm{lcm}(a, b) = \mathrm{lcm}(b, a)$

(2) $\mathrm{lcm}(a, b, c) = \mathrm{lcm}(\mathrm{lcm}(a, b), c)$

この定理の証明は省略する．

【定理 3.10】

$a, b, c \in \mathbb{Z}$ とし，$\gcd(a, b) = g$ とおく．このとき，次の 2 つの条件は同値である．

(i) $\exists x, y \in \mathbb{Z}$ s.t. $ax + by = c$

(ii) $g \mid c$

【証明】

(i) $\Rightarrow$ (ii)

ある整数 x, y があり，$ax + by = c$ となるとする．また，$\gcd(a, b) = g$ より，整数 q, q' が存在して，$a = gq, b = gq'$ とできる．よって，$c = ax + by = gqx + gq'y = g(qx + q'y)$ となり，$g \mid c$ である．

(i) $\Leftarrow$ (ii)

$ax + by$ の形で表される正の整数のうち最小のものを $k_0 = ax_0 + by_0$ とする．このとき，$k = ax + by$ とすると，k は k_0 の倍数である．なぜなら，もし，k が k_0 の倍数でないと仮定すると，ある整数 q, r があり，

$$k = k_0 q + r \qquad (0 < r < k_0)$$

と表される．このとき，

$$r = k - k_0 q = (ax + by) + (ax_0 + by_0)q = a(x + x_0 q) + b(y + y_0 q)$$

となり，k_0 より小さい $ax + by$ の形で表される正の整数が作れ，k_0 の最小性に矛盾する．よって，任意の $ax + by$ の形で表される整数は k_0 の倍数である．

$a = a \cdot 1 + b \cdot 0, b = a \cdot 0 + b \cdot 1$ はどちらも $ax + by$ の形で表される整数なので，k_0 の倍数である．よって，k_0 は a と b の公約数である．また (i) $\Rightarrow$ (ii) より，k_0 は g の倍数である．したがって，$k_0 = g$ となる．

ここで，$c = gp$ とすると，$c = dp = (ax_0 + by_0)p = ax_0 p + by_0 p$ となる．

□

【定理 3.11】

$a, b \in \mathbb{Z}, m \in \mathbb{Z}^+$ とする．このとき，次が成り立つ．

$$\gcd(ma, mb) = m \cdot \gcd(a, b)$$

【証明】

$\gcd(a, b) = g, \gcd(ma, mb) = g'$ とおく．$m \neq 0$ であることから，

$g \mid a, g \mid b$ とすると，$mg \mid ma, mg \mid mb$ である．よって，$mg \mid g'$ となる．

また，適当な $x, y \in \mathbb{Z}$ をとって，$g = ax + by$ とすると，$mg = max + mby$ となり，$g' \mid mg$ である．よって，$g' = mg$ となる．

□

$a, b \in \mathbb{Z}$ に対して，$\gcd(a, b) = 1$ となるとき，a と b は互いに素であるという．これを記号で $a \perp b$ と書く．

【定理 3.12】

$a, b, c \in \mathbb{Z}, a \perp b$ とする．このとき，$a \mid bc$ なら $a \mid c$ である．

【証明】

$a \perp b$ で $a \mid bc$ とする．$\gcd(a, b) = 1$ なので，ある整数 x, y が存在して，$ax + by = 1$ となる．両辺に c をかけて，

$$acx + bcy = c$$

$a \mid bc$ より，左辺は a の倍数である．よって，$a \mid c$ となる．

□

【定理 3.13】

$a, b, c \in \mathbb{Z}$ とする．このとき，

$$a \perp b \text{ かつ } a \perp c \Longleftrightarrow a \perp bc$$

【証明】

($\Rightarrow$)

$\gcd(a, bc) = g$ とおくと，$g \mid a, g \mid bc$ である．もし $\gcd(g, b) > 1$ ならば，$g \mid a$ より $\gcd(a, b) > 1$ となる．これは，$a \perp b$ に矛盾．よって，$\gcd(g, b) = 1$ であり，$g \mid c$ となる．$g \mid a$ なので g は a と c の公約数である．$a \perp c$ より $g = 1$ でないといけない．

($\Leftarrow$)

$\gcd(a, b) > 1 \Rightarrow \gcd(a, bc) > 1$ も $\gcd(a, c) > 1 \Rightarrow \gcd(a, bc) > 1$ も明らかである．よって，

$$\gcd(a, b) > 1 \text{ または } \gcd(a, c) > 1 \Longrightarrow \gcd(a, bc) > 1$$

対偶をとれば，

$$\gcd(a, bc) = 1 \Longrightarrow \gcd(a, b) = 1 \text{ かつ } \gcd(a, c) = 1$$

□

【定理 3.14】

$a, b \in \mathbb{Z}^+, \gcd(a, b) = g, \mathrm{lcm}(a, b) = l$ とする．このとき，

$$ab = gl$$

【証明】

$l = ab' = a'b$ とする．ab は a と b の公倍数であるので，ab は l の倍数となる．よって，$ab = lq$ とする．$l = ab' = a'b$ を代入して，$a = a'q, b = b'q$ を得る．よって，q は a と b の公約数である．なので，$g = qe$ とする．a, b は g で割り切れるので，a', b' は e で割り切れる．ここで，$a' = ea'', b' = eb''$ とおくと，$l = ab''e = a''be$ となる．もし，$e > 1$ であると仮定すると，$ab'' = a''b = d$ とすることで，d は a と b の公約数で，$d < l$ となる．これは，l の最小性に矛盾する．よって，$e = 1$ でなければならない．したがって，$q = g$ となる．

□

この定理は高校数学でも学ぶほど，有名な事実であるだろう．

3.4　素数と素因数分解

最後に紹介するのは素数である．これは，いまだに解決されていない問題も残っているほど，奥深く重要な概念である．

p を 1 より大きい整数とする．p の正の約数が 1 と p のみであるとき，p は素数であるという．また，そうでないときは合成数という．素数全体の集合を $\mathbb{P}$ と書く．

【定理 3.15】

$p \in \mathbb{P}, a, b \in \mathbb{Z}$ とする．このとき，

$$p \mid ab \Longrightarrow p \mid a \text{ または } p \mid b$$

【証明】

$\forall n \in \mathbb{Z}^+$ に対し，$p \perp n \Leftrightarrow p \nmid n$ であることに注意する．

$$a \perp b \text{ かつ } a \perp c \Longrightarrow a \perp bc$$

なので，

$$a \nmid b \text{ かつ } a \nmid c \Longrightarrow a \nmid bc$$

対偶をとれば，

$$p \mid ab \Longrightarrow p \mid a \text{ または } p \mid b$$

□

【定理 3.16】

n を 1 より大きい整数とする．このとき，n は素数の積として表せる．しかもその表し方は積の順序を除いて一意である．

【証明】

任意の素数がそうなることは自明なので，任意の合成数について，主張が正しいことを示す．まず，最も小さい合成数 $4 = 2 \times 2$ については正しい．ここで，任意の合成数 n に対し，n より小さい合成数では主張が正しいと仮定する．

n は合成数なので，

$$n = ab \qquad (a, b \in \mathbb{Z}, 1 < a, b < n)$$

とできる．いま，a, b は素数または n より小さい合成数になるので，a, b は素数の積で表される．よって，n も素数の積で表すことができる．

また，n を素数の積に分解して，

$$n = pp'p'' \cdots = qq'q'' \cdots$$

が得られたなら，$pp'p'' \cdots$ が素数 q で割り切れるので，$p, p', p'', \ldots$ の中に q で割り切れるものがある．いま，p が q で割り切れるとすれば，$p \in \mathbb{P}$ なので，$p = q$ となる．よって，

$$p'p'' \cdots = q'q'' \cdots$$

この数を m とすれば，m は素数または n より小さい合成数になるので，仮定より，二つの分解は一致している．よって，n に対する 2 つの分解も一致する．

□

整数 $n(>1)$ を素数の積で表すことを素因数分解という．また，n の約数となる素数を n の素因数という．

【定理 3.17】

素数は無数に存在する．

【証明】

$p_1, p_2, \ldots, p_n$ が素数だとする．いま，次のような数を考える．

$$a = p_1 p_2 \cdots p_n + 1$$

定理 3.16 より，a を割り切る素数 p が存在するはずである．しかし，$p_1, p_2, \ldots, p_n$ はどれも a を割り切らない．よって，p は $p_1, p_2, \ldots, p_n$ のどれでもない新たな素数である．ここで，新たな素数 p を加えて，$p_1, p_2, \ldots, p_n, p$ を素数だとすると，同様の議論で新たな素数 p' が作れる．これを繰り返すことで素数を無数に作ることができる．したがって，素数は無数に存在する．

□

最後の定理は，誰もが知っている事実ではないだろうか．整数論の本を読むと，必ずと言っていいほどこの定理の証明が書かれている．それほど，この定理は整数論にとって，基礎的で重要な事実なのである．ここで紹介したこと以外にも整数論では様々なことが分かっている．今までしてきたような純粋な議論だけでなく，様々な展開，応用がなされて研究されている．abc 予想や Riemann 予想などは，数学を専攻している人でなくても，知っているような有名な問題ではないだろうか．これらは整数論の問題である．

参考文献

[1] MATHEMATICS.PDF（2011）「数の構成自然数から複素数まで」
http://mathematics-pdf.com/pdf/construction_of_numbers.pdf
[2] 高木貞治（1931-2016）『初等整数論講義』共立出版