同値関係と商集合

ここから，自然数から出発し，整数，有理数，実数，複素数といったように数を構成してゆく話へと向かう．この構成作業のなかで便利に用いられるのが，「同値関係」の概念，およびそれに付随する「商集合」の概念である．本章ではこれらを説明し，またそれを用いて，整数と有理数の構成を実行する．

3.1 同値関係と商集合

●整数に対する合同式

同値関係の概念の一般的な定義に先立ち，その実例として，整数に対する「合同式」について説明しておきたい．

合同式とは次のようなものである．まず（1 以上の）自然数 m が与えられているとする．2 つの整数 a, b について，$a-b$ が m の倍数であるとき，a と b は m を**法** (modulus) として**合同** (congruent) であるといい，

$$a \equiv b \pmod{m} \tag{3.1}$$

と表す．たとえば

$$100 \equiv 1 \pmod{9}, \qquad -7 \equiv 9 \pmod{4}.$$

口頭で述べるときは「a と b は modulo m で合同である」という言い方もよく使われる．また式 (3.1) において，法 m を別途なんらかの形で明らかにしてあるときは，$(\mathrm{mod}\ m)$ は省略してもよい．

合同式の記法はよくできている．式 (3.1) は等式と似た格好をしているが，実際の性質の面から見ても等式と似ているところがあって，たとえば次の性質がある（ここで法 m は何でもよい）：

$$a \equiv b \text{ かつ } b \equiv c \ \Rightarrow\ a \equiv c. \tag{3.2}$$

つまり

$$2\cdot 7 \equiv 5\cdot 7 \ (\mathrm{mod}\ 3) \text{ かつ } 5\cdot 7 \equiv 5\cdot(-5) \ (\mathrm{mod}\ 3) \text{ だから，} 2\cdot 7 \equiv 5\cdot(-5) \ (\mathrm{mod}\ 3) \text{ である} \tag{3.3}$$

といった議論は正しい（もちろん途中で法を変更してはいけない）．もっと長くつなげてもよい：

$$\begin{aligned} 1\cdot 2\cdot 3\cdot 4 &\equiv 6\cdot 2\cdot 3\cdot 4 \pmod{5} \\ &\equiv 6\cdot 7\cdot 3\cdot 4 \pmod{5} \\ &\equiv 6\cdot 7\cdot 8\cdot 4 \pmod{5} \\ &\equiv 6\cdot 7\cdot 8\cdot 9 \pmod{5}, \\ \therefore\quad 1\cdot 2\cdot 3\cdot 4 &\equiv 6\cdot 7\cdot 8\cdot 9 \pmod{5}. \end{aligned} \tag{3.4}$$

性質 (3.2) は，関係 $\equiv$ の**推移律** (transitivity) と呼ばれる．

注 3.1. ちょっと口うるさい注意をするが，式 (3.4) のように合同式を書き連ねる記法自体，関係 $\equiv$ が推移律 (3.2) を満たすからこそ“許される”のである．推移律を満たさない場合に式 (3.4) のような書き方をするのは，意図がはっきりしなくなる恐れがあり良くない．たとえば（合同式とは全然関係ないが）

$$a \neq b \neq c$$

と書くとどうだろうか．「$a \neq b$」，「$b \neq c$」の 2 つが述べられていることは確実だが，書き手が「$a \neq c$」まで含めているのかどうかについては，意見は分かれるだろう．

合同式と通常の等式に共通する性質としては，もっと原始的なものもある．たとえば，任意の法 m について，どんな整数 $a \in \mathbb{Z}$ に対しても

$$a \equiv a \tag{3.5}$$

が成り立つ．これは関係 $\equiv$ の**反射律** (reflexiveness) である．また，任意の $a, b \in \mathbb{Z}$ に対して

$$a \equiv b \ \Rightarrow \ b \equiv a \tag{3.6}$$

も成り立つ．これは関係 $\equiv$ の**対称律** (symmetry) と呼ばれる．

反射律 (3.5)，対称律 (3.6)，推移律 (3.2) が成立することを指して，整数の関係 $\equiv$ は「同値関係」であるという言い方をする．では一般的な定義に移ろう．

●同値関係

「関係」という言葉を曖昧なまま使ってきたので，これをきちんと定義することから始める．

定義．集合 A 上の**関係** (relation) とは，直積 $A \times A$ の元に対する条件のことをいう．つまり，A 上の関係 R とは，各々の $(a, b) \in A \times A$ に対し命題（真偽の定まる言明）$R(a, b)$ を与えるようなものである．$R(a, b)$ のことを $a\,R\,b$ とも書く．

たとえば，m を自然数とするとき，「$a - b$ は m の倍数である」というのは確かに整数の組 $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ に対する条件だから，これは $\mathbb{Z}$ 上の関係である．この関係が $\equiv$ である（自然数 m に依存して決まる関係なので，正確を期すなら $\equiv_m$ のような記号を使うべきであろう）．上に述べた一般的な定義によれば，「$a - b$ は m の倍数である」というのを $\equiv(a, b)$ と書くこともできるわけだが，普通は $a \equiv b$ と書く．

そして，「同値関係」を次のように定義する．

定義．集合 A 上の関係 R が**同値関係** (equivalence relation) であるとは，任意の $a, b, c \in A$ に対して

$$a\,R\,a \qquad (\textbf{反射律}), \tag{3.7a}$$

$$a\,R\,b \ \Rightarrow \ b\,R\,a \qquad (\textbf{対称律}), \tag{3.7b}$$

$$a\,R\,b \text{ かつ } b\,R\,c \ \Rightarrow \ a\,R\,c \quad (\textbf{推移律}) \tag{3.7c}$$

が成り立つことをいう．R が同値関係であるとき，$a, b \in A$ について $a\,R\,b$ が成り立つならば，そのことを指して，a, b は同値関係 R に関して**同値** (equivalent) であるという．

同値関係を表すときは，$\sim$ や $\equiv$ といった記号を使うことが多い．

もちろん，m を法とする合同 $\equiv$ は $\mathbb{Z}$ 上の同値関係である．他にもいろいろな例がある．すぐに説明できる例を 2 つ提示しておく．

例 3.2. $a, b \in \mathbb{R}$ に対し $a \sim b \overset{\text{def}}{\Leftrightarrow} a - b \in \mathbb{Z}$ と定めれば，$\sim$ は $\mathbb{R}$ 上の同値関係である．

例 3.3. V を線型空間（ベクトル空間），W をその部分空間とする．そのとき，$\boldsymbol{x}, \boldsymbol{y} \in V$ に対し $\boldsymbol{x} \sim \boldsymbol{y} \overset{\text{def}}{\Leftrightarrow} \boldsymbol{x} - \boldsymbol{y} \in W$ と定めれば，$\sim$ は V 上の同値関係である．

さて，同値関係があると，次に述べる「同値類」というものを考えることができる．

定義．集合 A 上に同値関係 $\sim$ が与えられているとする．そのとき，各元 $a \in A$ に対し，a の属する**同値類** (equivalence class) とは

$$\{\, x \in A \mid x \sim a \,\}$$

という A の部分集合のことである．これを $[a]$ という記号で表す．

任意の $a, b \in A$ に対して，$a \sim b$ は $[a] = [b]$ となるための必要十分条件である（問題 3.5 (1)）．同値類の概念を導入することにより，$a \sim b$ という幾分緩やかさを残した関係性を，$[a] = [b]$ という揺るぎない等式に移し替えることができるのである．

●整数の合同式と演算．剰余類の演算とその well-definedness

整数の合同式に話を戻そう．

整数には加法 $+$，乗法 $\times$ という 2 つの重要な演算があるが（減法は加法の逆演算だから，あえて別物として取りあげなくてもよいだろう），合同式はこれらの演算に関して，次のような性質を持つ．

命題 3.4. 任意の $a, b, c, d \in \mathbb{Z}$ について次が成り立つ．

$$a \equiv c \text{ かつ } b \equiv d \ \Rightarrow\ a+b \equiv c+d, \tag{3.8a}$$
$$a \equiv c \text{ かつ } b \equiv d \ \Rightarrow\ ab \equiv cd. \tag{3.8b}$$

ただし法 m は任意である．

証明は簡単だと思うので演習問題とする（問題 3.2）．たとえば式 (3.8b) の証明は，(3.3) を一般的な形に書き直せば得られる．

例 3.5. 命題 3.4 を用いて，123456789 を 11 で割った余りを求めてみよう．まず，$10 \equiv -1 \pmod{11}$．したがって (3.8b) を繰り返し使うことにより，任意の $k \in \mathbb{N}$ について $10^k \equiv (-1)^k \pmod{11}$ である．ゆえに 11 を法として

$$\begin{aligned} 123456789 &\equiv 1\cdot 10^8 + 2\cdot 10^7 + 3\cdot 10^6 + 4\cdot 10^5 + 5\cdot 10^4 + 6\cdot 10^3 + 7\cdot 10^2 + 8\cdot 10^1 + 9\cdot 10^0 \\ &\equiv 1\cdot 1 + 2\cdot(-1) + 3\cdot 1 + 4\cdot(-1) + 5\cdot 1 + 6\cdot(-1) + 7\cdot 1 + 8\cdot(-1) + 9\cdot 1 \\ &\equiv 1-2+3-4+5-6+7-8+9 \equiv 5. \end{aligned}$$

これは $123456789 - 5$ が 11 で割り切れることを意味する．ゆえに，123456789 を 11 で割った余りは 5 になる．

ここで，命題 3.4 を整数の合同 $\equiv$ に関する同値類（これを整数の**剰余類**と呼ぶ）の概念を用いて解釈してみたい．前項の最後に指摘したように $a \equiv c$ は $[a] = [c]$ と同値だから，たとえば (3.8a) は次のように表すことができる：

$$[a] = [c] \text{ かつ } [b] = [d] \ \Rightarrow\ [a+b] = [c+d]. \tag{3.9}$$

これは，整数 $a, b \in \mathbb{Z}$ に対して剰余類 $[a+b]$ を考えるとき，次のような現象が起こっていることを示している（括弧【】内を副音声のようなものと思って読んでください）．

> a, b を別の整数に変更したとしても【それらを c, d としよう】
> 剰余類 $[a]$, $[b]$ が変わらないのであれば【つまり $[a] = [c]$, $[b] = [d]$ なのであれば】
> 剰余類 $[a+b]$ も変わらない【$[a+b] = [c+d]$ である】．

一言で言えば，剰余類 $[a+b]$ は $a, b \in \mathbb{Z}$ の剰余類 $[a]$, $[b]$ にしか依存しない．そこでわれわれは $[a+b]$ を剰余類 $[a]$, $[b]$ の**和**と呼ぶことができ，次のように書き表すことができる：

$$[a] + [b] = [a+b]. \tag{3.10}$$

もし仮に $[a+b]$ が $[a]$, $[b]$ だけで決まらなかったとしたら，それを「$[a]$, $[b]$ の○○」と呼ぶわけにはいかない．式 (3.8a)，もしくはその言い換えにあたる式 (3.9) が，「$[a]$, $[b]$ の和」の定義の正当性を，別の言葉で言えば well-definedness を保証しているのである．

式 (3.8a) を式 (3.9) に書き換えたのと同様に，式 (3.8b) は

$$[a] = [c] \text{ かつ } [b] = [d] \ \Rightarrow\ [ab] = [cd] \tag{3.11}$$

と書き換えられる．そしてこちらは，剰余類の**積** $[a][b]$ が

$$[a][b] = [ab] \tag{3.12}$$

によって well-defined に定義されることを示している．

●商集合

前項で見たように，同値関係を備えた集合 A にある種の演算が定義されているとき，それが同値類たちの間の演算を引き起こすことがある．そこで，すべての同値類を集めて得られる集合に名前を付けておくと便利である．

定義. 集合 A 上に同値関係 $\sim$ が与えられているとき，各元の属する同値類全体の集合

$$\{\,[a] \mid a \in A\,\}$$

のことを，A の $\sim$ による**商集合** (quotient set) といい，記号 $A/\!\sim$ で表す.

例として再び，整数の m を法とする合同 $\equiv$ について考えてみよう．$\mathbb{Z}$ の $\equiv$ に関する同値類は全部で m 個あり，それらはしばしば，$\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{m-1}$ という記号で表される：

$$\begin{aligned}
\overline{0} &= \{\ \ldots,\ -2m,\ -m,\ \boxed{0},\ m,\ 2m,\ \ldots\ \},\\
\overline{1} &= \{\ \ldots,\ -2m+1,\ -m+1,\ \boxed{1},\ m+1,\ 2m+1,\ \ldots\ \},\\
\overline{2} &= \{\ \ldots,\ -2m+2,\ -m+2,\ \boxed{2},\ m+2,\ 2m+2,\ \ldots\ \},\\
&\ \ \vdots\\
\overline{m-1} &= \{\ \ldots,\ -m-1,\ -1,\ \boxed{m-1},\ 2m-1,\ 3m-1,\ \ldots\ \}.
\end{aligned}$$

これについて商集合は

$$\mathbb{Z}/\!\equiv\ = \{\,\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{m-1}\,\}$$

となる．この商集合は，通常 $\mathbb{Z}/m\mathbb{Z}$ という記号で表される．前項では，$\mathbb{Z}/m\mathbb{Z}$ に加法や乗法が定義されることを見たのである.

上の例では，各々の同値類 $\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{m-1}$ は，$\mathbb{Z}$ の部分集合として，どの 2 つも互いに交わりを持たず，そしてすべての和集合は $\mathbb{Z}$ に一致している．このことはどんな同値関係についても成り立つ.

命題 3.6. 集合 A 上に同値関係 $\sim$ が与えられているとする．そのとき，任意の $a, b \in A$ に対し，もし $[a] \neq [b]$ ならば $[a] \cap [b] = \emptyset$ である．また，$\bigcup_{a \in A} [a] = A$ である.

後半は $a \in [a]$ より明らか．前半について，$[a] = [b]$ は $a \sim b$ と同値だったので，示すべきことは $a \not\sim b$ ならば $[a] \cap [b] = \emptyset$ となることである．これは演習問題とする（問題 3.5 (2)）.

なお一般に，集合 A 上に同値関係 $\sim$ が与えられているとき，$a \in A$ を同値類 $[a] \in A/\!\sim$ に移すことにより，全射 $\pi\colon A \to A/\!\sim$ を定めることができる．この π はふつう**自然な全射**と呼ばれる.

3.2 整数の構成，有理数の構成

この節では次の 2 つのことを行う.

(1) 自然数をもとにして整数を構成する.
(2) 整数をもとにして有理数を構成する.

(1) においては，いったん表向きには「整数」の概念のことを忘れ，自然数しか知らないふりをして，自然数全体の集合 $\mathbb{N}$ から，これまでに学んだ集合論的手続きだけを用いて，「整数全体の集合」と呼ぶべき集合 $\mathbb{Z}$ を構成し，またその上の演算をうまく定義する．(2) でも同様に，表向きには「有理数」の概念のことを忘れ，整数全体の集合 $\mathbb{Z}$ から，「有理数全体の集合」と呼ぶべき集合 $\mathbb{Q}$ を構成し，その上の演算をうまく定義するのである.

●整数の構成

本項では便宜上 $\mathbb{N} = \{\,0, 1, 2, 3, \ldots\,\}$ としておく.

$\mathbb{N}$ から $\mathbb{Z}$ を構成するにあたり着目するのは，減法という演算である．減法が $\mathbb{N}$ では自由にはできなかったのに，$\mathbb{Z}$ では自由にできるようになっている——整数とは減法を自由に行うために生まれた数概念だと言ってもよい.

$\mathbb{N}$ の元から引き算によって得られるような数の全体を考えれば，それが「整数全体の集合」である．だがわれわれは，結果が負の数になるような引き算は知らないふりをしなければならない．そこでどうするかというと，自然数の対 (m, n) によって新たな数を表現するのである——内心では「$m - n$」という差のつもりで.

ところで，対 (m,n) が実際には「$m-n$」を表すのだとすれば，異なる対であっても，実際には同じ数を表していると考えられるべきものもある．たとえば，$(2,5)$ と $(4,7)$ は同じ数を表すと見なすべきだ（心の中で $2-5$ と $4-7$ を計算しながら）．一般に，2 つの対 (m,n) と (m',n') の表す数は，

$$m+n'=m'+n$$

のときに同じものとされるべきである（心の中で——これは「$m-n=m'-n'$」の同値な言い換えになっているな，よし）．ここで登場するのが，同値関係と商集合の考えである．対 (m,n) そのものを数と考えるのではなく，適切な同値関係を導入して，(m,n) の属する同値類を数と考えることにするのである．

対 (m,n) たちのなす集合 $\mathbb{N}\times\mathbb{N}$ において，われわれは，次のように関係 $\sim$ を定義する．

$$(m,n)\sim(m',n') \overset{\text{def}}{\Leftrightarrow} m+n'=m'+n. \tag{3.13}$$

補題 3.7. 式 (3.13) で定義した関係 $\sim$ は，$\mathbb{N}\times\mathbb{N}$ 上の同値関係である．

［証明］ 反射律 (3.7a) および対称律 (3.7b) の成立は明らか．推移律 (3.7c) が成り立つことを確認しよう．$(m,n)\sim(m',n')$, $(m',n')\sim(m'',n'')$ と仮定すると，定義によって $m+n'=m'+n$, $m'+n''=m''+n'$ だから，辺々加え合わせて

$$m+n'+m'+n''=m'+n+m''+n'.$$

両辺から $m'+n'$ を引いて

$$m+n''=m''+n,$$

すなわち $(m,n)\sim(m'',n'')$ が得られる．これで推移律も示された． □

補題 3.7 によって，われわれは，次のようにして「整数全体の集合」$\mathbb{Z}$ をつくることができる．

定義. 商集合 $(\mathbb{N}\times\mathbb{N})/\!\sim$ のことを $\mathbb{Z}$ で表し，その元のことを**整数**と呼ぶ．各 $m\in\mathbb{N}$ に対し，対 $(m,0)$ の属する同値類 $[(m,0)]\in\mathbb{Z}$ を，自然数 m と同一視する．これによって $\mathbb{N}$ は $\mathbb{Z}$ の部分集合と見なされる．

さて，$\mathbb{Z}$ における演算はどのように定義したらいいだろうか．(m,n) の属する同値類 $[(m,n)]$ は，内心では「$m-n$」という数のつもりなのであった．したがって，$[(m,n)]$, $[(m',n')]$ の「和」は

$$(m-n)+(m'-n')=(m+m')-(n+n')$$

という数であるべきだし，「積」は

$$(m-n)(m'-n')=(mm'+nn')-(mn'+m'n)$$

という数であるべきだ．これらを定義とするにあたっては，前節で整数の剰余類の演算を定義したときと同じように well-definedness の問題があるのだが，いったんそのことは置いておいて，定義を述べてしまおう．

定義. $\mathbb{Z}=(\mathbb{N}\times\mathbb{N})/\!\sim$ の元 $[(m,n)]$, $[(m',n')]$ に対して，$[(m+m',n+n')]$ をそれらの**和**と呼ぶ．また，$[(mm'+nn',mn'+m'n)]$ をそれらの**積**と呼ぶ．

この定義の well-definedness を確かめるには，たとえば和に関しては

> (m,n), (m',n') を別の対に変更したとしても【それらを (m_1,n_1), (m_1',n_1') としよう】
> 同値類 $[(m,n)]$, $[(m',n')]$ が変わらないのであれば【つまり $[(m,n)]=[(m_1,n_1)]$, $[(m',n')]=[(m_1',n_1')]$ なのであれば】
> 同値類 $[(m+m',n+n')]$ も変わらない【$[(m+m',n+n')]=[(m_1+m_1',n_1+n_1')]$ である】

ということをチェックする必要がある．積についても同様である．同値類の一致 $[(m,n)]=[(m_1,n_1)]$ が成立するための必要十分条件が $(m,n)\sim(m_1,n_1)$ だったことを思い出すと，証明すべきものは次の補題である．

補題 3.8. 任意の (m,n), (m',n'), (m_1,n_1), $(m_1',n_1') \in \mathbb{N}\times\mathbb{N}$ について，もし $(m,n)\sim(m_1,n_1)$ かつ $(m',n')\sim(m_1',n_1')$ ならば，次が成り立つ．

$$(m+m',n+n')\sim(m_1+m_1',n_1+n_1'), \tag{3.14a}$$
$$(mm'+nn',mn'+m'n)\sim(m_1m_1'+n_1n_1',m_1n_1'+m_1'n_1). \tag{3.14b}$$

［証明］ 証明を簡単にするために，まず，$(m',n')=(m_1',n_1')$ と仮定して証明すれば十分であることを指摘しておく．すなわち，$(m,n)\sim(m_1,n_1)$ という仮定のもとで次を示せばよい．

$$(m+m',n+n')\sim(m_1+m',n_1+n'), \tag{3.15a}$$
$$(mm'+nn',mn'+m'n)\sim(m_1m'+n_1n',m_1n'+m'n_1). \tag{3.15b}$$

なぜなら，たとえば (3.15a) がわかっていれば，(3.14a) は

$$\begin{aligned}(m+m',n+n')&\sim(m_1+m',n_1+n')\sim(m'+m_1,n'+n_1)\\&\sim(m_1'+m_1,n_1'+n_1)\sim(m_1+m_1',n_1+n_1')\end{aligned}$$

として示されるからである．同様にして (3.15b) から (3.14b) が従う．

(3.15a) の証明．仮定により $m+n_1=m_1+n$ であるから

$$(m+m')+(n_1+n')=(m+n_1)+(m'+n')=(m_1+n)+(m'+n')=(m_1+m')+(n+n').$$

ゆえに $(m+m',n+n')\sim(m_1+m_1',n_1+n')$.

(3.15b) の証明．仮定により $m+n_1=m_1+n$ であるから

$$\begin{aligned}(mm'+nn')+(m_1n'+m'n_1)&=(m+n_1)m'+(m_1+n)n'\\&=(m_1+n)m'+(m+n_1)n'=(m_1m'+n_1n')+(mn'+m'n).\end{aligned}$$

ゆえに $(mm'+nn',mn'+m'n)\sim(m_1m'+n_1n',m_1n'+m'n_1)$. □

これで $\mathbb{Z}$ における和と積が定義できた．さらにこの演算の満たす諸性質を確認すべきなのだが，その証明はある程度単純作業なので，省略してしまうことにしよう．結論は以下のとおりである．（一部を演習問題とする．問題 3.6.）

命題 3.9. 整数の演算について次の性質が成り立つ．

(i) 和について次の性質が成り立つ．
  (a) 任意の a, b, $c\in\mathbb{Z}$ について $(a+b)+c=a+(b+c)$（**和の結合律**）．
  (b) 任意の a, $b\in\mathbb{Z}$ について $a+b=b+a$（**和の交換律**）．
  (c)「任意の $a\in\mathbb{Z}$ について $a+0=a$」という性質を持つ元 $0\in\mathbb{Z}$ がただ一つ存在する（**零元の存在**）．
  (d) 任意の $a\in\mathbb{Z}$ について，$a+b=0$ という性質を持つ元 $b\in\mathbb{Z}$ がただ一つ存在する（**和に関する逆元の存在**）．この b を $-a$ と表す．

(ii) 積について次の性質が成り立つ．
  (a) 任意の a, b, $c\in\mathbb{Z}$ について $(ab)c=a(bc)$（**積の結合律**）．
  (b) 任意の a, $b\in\mathbb{Z}$ について $ab=ba$（**積の交換律**）．
  (c)「任意の $a\in\mathbb{Z}$ について $1a=a$」という性質を持つ元 $1\in\mathbb{Z}$ がただ一つ存在する（**単位元の存在**）．

(iii) 和と積について次の性質が成り立つ．
  (a) 任意の a, b, $c\in\mathbb{Z}$ について $(a+b)c=ac+bc$（**分配律**）．

（以上のことを指して，「整数全体の集合 $\mathbb{Z}$ は単位元を持つ可換環である」と言う．）

●有理数の構成

整数をもとにした有理数の構成も，基本的には前項と同じようにして行われる．

$\mathbb{N}$ から $\mathbb{Z}$ を構成するときは減法という演算に着目したのだが，$\mathbb{Z}$ から $\mathbb{Q}$ を構成するために着目する演算は除法である．有理数とは除法を自由に行うために生まれた数概念である．

そこで，$\mathbb{Z}$ の元から割り算によって得られるような数の全体を考えれば，それが「有理数全体の集合」である．もちろんわれわれは，結果が整数にならない割り算は知らないふりをするのだから，$b \neq 0$ を満たす整数の対 (a, b) が新たな数を表現するものと考える——内心では「a/b」という商のつもりで．

一般に，2 つの対 (a, b) と (a', b') の表す数は，

$$ab' = a'b$$

のときに同じものとされるべきである（心の中で——これは「$a/b = a'/b'$」の同値な言い換えになっている）．

そこで対 (a, b) たちのなす集合 $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ において，次のように関係 $\sim$ を定義する．

$$(a, b) \sim (a', b') \overset{\text{def}}{\Leftrightarrow} ab' = a'b. \tag{3.16}$$

この後の進行はさっきとだいたい同じである．概略を示し，詳細は読者に任せる．（一部を演習問題とする．問題 3.7.）

補題 3.10. 式 (3.16) で定義した関係 $\sim$ は，$\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ 上の同値関係である．

定義. 商集合 $(\mathbb{Z} \times (\mathbb{Z} \setminus \{0\}))/\sim$ のことを $\mathbb{Q}$ で表し，その元のことを**有理数**と呼ぶ．対 (a, b) の属する同値類 $[(a, b)]$ のことを a/b という記号で表す．特に，$a/1$ を $a \in \mathbb{Z}$ と同一視する．これによって $\mathbb{Z}$ は $\mathbb{Q}$ の部分集合と見なされる．

演算は次のようにして定義される．

定義. $\mathbb{Q} = (\mathbb{Z} \times (\mathbb{Z} \setminus \{0\}))/\sim$ の元 $[(a, b)]$, $[(a', b')]$ に対して，$[(ab' + a'b, bb')]$ をそれらの**和**と呼ぶ．また，$[(aa', bb')]$ をそれらの**積**と呼ぶ．

命題 3.11. 有理数全体の集合 $\mathbb{Q}$ は単位元を持つ可換環（命題 3.9 を参照）である．さらに次が成り立つ．

(ii) 積について次の性質が成り立つ．
  (d) 0 でない任意の $p \in \mathbb{Q}$ に対して，$pq = 1$ を満たす元 $q \in \mathbb{Q}$ がただ一つ存在する（**積に関する逆元の存在**）．この q を p^{-1} と表す．

（以上のことを指して，「有理数全体の集合 $\mathbb{Q}$ は体である」と言う．）

演習問題

3.1 「123456789 を 7 で割った余りはいくつか」という問題に対して，次のように答えることができることが知られている．

$123 - 456 + 789 = 456$ で，456 を 7 で割った余りは 1 だから，123456789 を 7 で割った余りも 1 である．

これが正しい理由を説明せよ．（ヒント：例 3.5 を参考にせよ．1001 は 7 の倍数.）

3.2 命題 3.4 を証明せよ．

3.3 $a, b, k \in \mathbb{Z}$ に対し，$ka \equiv kb \pmod{m}$ であるとする．

(1) もし k と m が互いに素であるならば，$a \equiv b \pmod{m}$ である．このことを証明せよ．

(2) k と m が互いに素でなければ，$a \equiv b \pmod{m}$ は一般には成立しない．反例を挙げよ．

3.4 p を素数とし，$a \in \mathbb{Z}$ は p の倍数ではないと仮定する．

(1) p 個の整数 $a \cdot 0, a \cdot 1, a \cdot 2, \ldots, a(p-1)$ からどの 2 つを選んでも，それらは p を法として合同ではないことを証明せよ．

(2)　$(a\cdot 1)\cdot(a\cdot 2)\cdot\cdots\cdot(a(p-1))\equiv 1\cdot 2\cdot\cdots\cdot(p-1) \pmod p$ を示せ．またそれを用いて，$a^{p-1}\equiv 1 \pmod p$ を示せ（**Fermat の小定理**）．（ヒント：問題 3.3.）

3.5　集合 A 上に同値関係 $\sim$ が与えられているものとする．次を証明せよ．

(1)　$a\sim b$ は $[a]=[b]$ であるための必要十分条件である．

(2)　$a\not\sim b$ ならば $[a]\cap[b]=\emptyset$.

3.6　整数に対する積の結合律（命題 3.9 の (ii) (a)）を証明せよ．

3.7　有理数の和が well-defined であることを確かめるには何を証明すればいいか述べ，それを証明せよ．

3.8　V を体 K 上の線型空間（ベクトル空間）とし，W をその部分空間とする．例 3.3 で行ったように，$\boldsymbol{x},\boldsymbol{y}\in V$ に対し $\boldsymbol{x}\sim\boldsymbol{y}\overset{\text{def}}{\Leftrightarrow}\boldsymbol{x}-\boldsymbol{y}\in W$ と定めることにより同値関係 $\sim$ を定義する．この同値関係に関する商集合を考えよう．慣習に従い，$V/\!\sim$ と書く代わりに V/W と書く．V/W における和とスカラー倍を以下のようにして定める．

$$\begin{aligned}[\boldsymbol{x}]+[\boldsymbol{y}]&=[\boldsymbol{x}+\boldsymbol{y}], &&\boldsymbol{x},\ \boldsymbol{y}\in V,\\ c[\boldsymbol{x}]&=[c\boldsymbol{x}], &&\boldsymbol{x}\in V,\ c\in K.\end{aligned}$$

これらが well-defined であることを確かめよ．（これらの演算によって V/W は線型空間となる．これを V の W による**商線型空間**という．）

3.9　$M(m,n)$ を $m\times n$ 行列全体の集合とする．$A,\,B\in M(m,n)$ に対し

$$A\sim B\ \overset{\text{def}}{\Leftrightarrow}\ B=PAQ \text{ となるような正則行列 } P,\,Q \text{ が存在する}$$

と定めることにより関係 $\sim$ を定義する（ただしもちろん，P は $m\times m$ 行列，Q は $n\times n$ 行列）．

(1)　$\sim$ が $M(m,n)$ 上の同値関係であることを証明せよ．

(2)　商集合 $M(m,n)/\!\sim$ は何個の元からなるか．

3.10　例 3.2 では，$a,\,b\in\mathbb{R}$ に対し $a\sim b\overset{\text{def}}{\Leftrightarrow}a-b\in\mathbb{Z}$ と定めることにより $\mathbb{R}$ 上の同値関係 $\sim$ を定義した．商集合 $\mathbb{R}/\!\sim$ についてよく理解するために，次のように，$\mathbb{R}/\!\sim$ と別の集合の間の全単射を 2 通り考えてみよう．

$$\begin{aligned}&f\colon\mathbb{R}/\!\sim\to[0,1), && [a]\mapsto(a\text{ の小数部分}),\\ &g\colon\mathbb{R}/\!\sim\to S^1=\{\,(x,y)\in\mathbb{R}^2\mid x^2+y^2=1\,\}, && [a]\mapsto(\cos(2\pi a),\sin(2\pi a)).\end{aligned}$$

(1)　$f,\,g$ が well-defined であることを説明せよ．

(2)　g には，f にはない利点がある．それを一つ指摘せよ．