商集合と代数的構造

前章では同値関係と商集合について学んだ．その際，“もとの集合”が代数的演算を備えた集合であるケースでは，商集合にも往々にして何らかの代数的演算が定義されることを，$\mathbb{Z}/m\mathbb{Z}$ をはじめとするいくつかの実例を通じて，われわれは見た．

本章ではこのような現象（の一部）について，もっと一般的な形で理解する．またその応用として，複素数の構成法について学ぶ．

4.1 可換環とその剰余環

本節では「剰余環」の概念について一般的な説明を行う．その基本的な例は，整数の剰余類からなる集合 $\mathbb{Z}/m\mathbb{Z} = \{\,\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{m-1}\,\}$ である．

●復習——$\mathbb{Z}/m\mathbb{Z}$ とその演算

正の整数 m に対し，m を法とする整数の剰余類とは，次のように $\mathbb{Z}$ 上の同値関係 $\equiv$ を定めたときの同値類のことだった（左辺では「$(\mathrm{mod}\ m)$」は省略している）：

$$a \equiv b \overset{\text{def}}{\Leftrightarrow} a - b \text{ は } m \text{ の倍数.} \tag{4.1}$$

m を法とする整数の剰余類は全部で m 個ある．各々の剰余類は（たとえば）0, 1, 2, …, $m-1$ という整数によって代表される．それらをわれわれは，それぞれ $\overline{0}$, $\overline{1}$, $\overline{2}$, …, $\overline{m-1}$ という記号で表していた．つまり

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

$\mathbb{Z}$ の $\equiv$ による商集合 $\mathbb{Z}/\equiv$ とは $\{\,\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{m-1}\,\}$ のことで，それを $\mathbb{Z}/m\mathbb{Z}$ とも書くのだった．

$\mathbb{Z}$ には加法 $+$ と乗法 $\times$ という演算があるが，$\mathbb{Z}/m\mathbb{Z}$ にも加法と乗法がある．それらは次のようにして定義された．整数 a の属する剰余類を $[a]$ と書くが，この記法を用いて，2 つの剰余類 $[a]$, $[b]$ が与えられたとき

$$[a] + [b] = [a+b], \qquad [a][b] = [ab] \tag{4.2}$$

と定める．ただし与えられた剰余類を $[a]$ のような形で書き表す方法は一意的ではないので，式 (4.2) によって和 $[a]+[b]$ や積 $[a][b]$ が well-defined に定義されているのかということを検討する必要がある．その well-definedness は，次の命題を証明することによって示されるのだった．

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

$$a \equiv c \text{ かつ } b \equiv d \ \Rightarrow\ a + b \equiv c + d, \tag{4.3a}$$

$$a \equiv c \text{ かつ } b \equiv d \ \Rightarrow\ ab \equiv cd. \tag{4.3b}$$

●なぜ $\mathbb{Z}/m\mathbb{Z}$ の演算は well-defined なのか

「なぜ $\mathbb{Z}/m\mathbb{Z}$ の演算は well-defined なのか」という問いについて，言い換えれば「なぜ命題 3.4 が成り立つのか」という問いについて，より深く考えてみたい．

これは実は，整数の合同という同値関係が，ある種の特徴的な方法で定義されていることに起因しているのである．

その特徴的な方法というのはこういうことだ．m の倍数全体の集合 $\{\, km \mid k \in \mathbb{Z} \,\}$ を通常 $m\mathbb{Z}$ と書くが（$\mathbb{Z}m$ と書くこともある），この記法を用いると，整数の合同の定義 (4.1) は

$$a \equiv b \overset{\text{def}}{\Leftrightarrow} a - b \in m\mathbb{Z} \tag{4.4}$$

と表すことができる．ところで (4.1) と (4.4) の違いは，単なる言葉遣いの問題だろうか．そうではない——というのがここでの見方である．(4.4) は，整数の合同が「$a-b$ がある特定の集合（ここでは $m\mathbb{Z}$）に属しているか否か」によって定義されていることを明確に表している．

では，$m\mathbb{Z}$ の代わりにどんな集合を考えても，同じように加法と乗法の定義された商集合が得られるだろうか．おそらく誰もが予期するとおり，そういうわけにはいかない．まず，そもそも，同値関係が定義されるために必要な条件がある．

命題 4.1. A を $\mathbb{Z}$ の部分集合とする．そのとき，

$$a \mathrel{R} b \overset{\text{def}}{\Leftrightarrow} a - b \in A$$

によって定義された関係 R が同値関係であるためには，次の (i), (ii), (iii) が成り立つことが必要十分である．

(i) $0 \in A$，　(ii) $x \in A$ ならば $-x \in A$，　(iii) $x, y \in A$ ならば $x + y \in A$.

［証明］ 関係 R が同値関係であるというのは，反射律，対称律，推移律が成り立つということだった．これらの 3 つの条件に，命題の条件 (i), (ii), (iii) がそれぞれ対応する．

まず反射律について考える．反射律とは任意の $a \in \mathbb{Z}$ に対して $a \mathrel{R} a$ ということだが，ある $a \in \mathbb{Z}$ について $a \mathrel{R} a$ であるならば，関係 R の定義によって $a - a \in A$，すなわち $0 \in A$ が従う．逆に $0 \in A$ ならば任意の $a \in \mathbb{Z}$ に対して $a \mathrel{R} a$ である．よって，反射律の成立は (i) と同値である．

次に対称律について．仮に対称律が成り立つとすれば，$a \mathrel{R} b$ のとき $b \mathrel{R} a$ でもある．したがって，もし $x \in A$ ならば，定義より直ちに $x \mathrel{R} 0$ だから，$0 \mathrel{R} x$ でもあることになって，$-x \in A$ がわかる．すなわち (ii) が得られる．逆に (ii) が成立すれば，$a \mathrel{R} b$ のとき $a - b \in A$ であることから $b - a \in A$ となり，$b \mathrel{R} a$ が従う．

最後に推移律について．仮に推移律が成り立つとすれば，$x, y \in A$ のとき $(x + y) \mathrel{R} x$, $x \mathrel{R} 0$ であることから $(x + y) \mathrel{R} 0$ となり，$x + y \in A$ が従う．つまり (iii) が得られる．逆に (iii) が成り立てば，$a \mathrel{R} b$, $b \mathrel{R} c$ のとき $a - b$, $b - c \in A$ であることから $a - c = (a - b) + (b - c) \in A$ となり，$a \mathrel{R} c$ がわかる． □

注 4.2. ここでは R という記号は $=, \leq, \geq, \ldots$ といった記号の仲間なので（関係演算子という），理屈の上では $(x+y) \mathrel{R} x$ と書かずに $x + y \mathrel{R} x$ と書いてもかまわないのだが，誤解を防ぐために括弧を付けた．

命題 4.1 により定義された同値関係について，さらに同値類の間の加法，乗法が well-defined に定義されるための条件を調べる．つまり，命題 3.4 に示されているような性質が成り立つための条件である．

命題 4.3. A を命題 4.1 の条件 (i), (ii), (iii) を満たす $\mathbb{Z}$ の部分集合とし，

$$a \sim b \overset{\text{def}}{\Leftrightarrow} a - b \in A$$

によって定義される同値関係 $\sim$ を考える．このとき，もし

(iv) $x \in A$, $a \in \mathbb{Z}$ ならば $ax \in A$

が成り立っているならば，任意の a, b, c, $d \in \mathbb{Z}$ について

$$a \sim c \text{ かつ } b \sim d \;\Rightarrow\; a + b \sim c + d, \tag{4.5a}$$
$$a \sim c \text{ かつ } b \sim d \;\Rightarrow\; ab \sim cd \tag{4.5b}$$

が成り立つ．

実は，(4.5a) のほうは (iv) がなくても成り立つ（確かめよ）．問題は (4.5b) のほうにある．

［命題 4.3 の証明］ 上で注意したことから，(4.5b) の成立だけを確かめればよい．$a \sim c$, $b \sim d$ であるとする．同値関係 $\sim$ の定義により，これは $a-c$, $b-d \in A$ を意味する．ここで

$$ab - cd = b(a-c) + c(b-d)$$

であるが，(iv) が成り立つのだから，$a-c$, $b-d \in A$ より $b(a-c)$, $c(b-d) \in A$．したがって (iii) より $b(a-c)+c(b-d) \in A$ でもあるので，$ab \sim cd$ であることがわかる．これで (4.5b) が示された． □

注 4.4. 命題 4.3 における条件 (iv) は目的のためには強すぎないかという心配をする人もいるかもしれない．実は，(iv) は (4.5b) が成立するために必要でもある．これは演習問題としよう（問題 4.1）．

まとめると，$\mathbb{Z}/m\mathbb{Z}$ という商集合が問題なく定まり，$\mathbb{Z}/m\mathbb{Z}$ において加法と乗法が無事に定義されたのは，$m\mathbb{Z}$ という集合を A としたとき，この A が命題 4.1，命題 4.3 にある条件 (i), (ii), (iii), (iv) を満たしていたからだったのである．なお，条件 (ii) は (iv) から従うので，実質的には (i), (iii), (iv) があればよいことに注意しよう．この観察によりわれわれは，「イデアル」の概念に導かれる．

●可換環，イデアル，剰余環

命題 3.9 では整数の演算に関する諸性質を述べたが，それらをまとめて一言で「$\mathbb{Z}$ は単位元を持つ可換環である」と表現したことを思い出そう．その意味を再度確認すると次のとおりである．以下では簡単のため，「可換環」と言ったら常に単位元を持つものと約束し，「単位元を持つ」はいちいち断らないことにする．

定義. 集合 R が加法と乗法と呼ばれる演算を備えており，次の性質が成り立つとき，R は（単位元を持つ）**可換環** (commutative ring) であるという．

(i) 加法について次の性質が成り立つ．
  (a) 任意の a, b, $c \in R$ について $(a+b)+c = a+(b+c)$.
  (b) 任意の a, $b \in R$ について $a+b = b+a$.
  (c)「任意の $a \in R$ について $a+0=a$」という性質を持つ元 $0 \in R$ が存在する（**零元**と呼ぶ）.
  (d) 任意の $a \in R$ について，$a+b=0$ を満たす元 $b \in R$ が存在する（この b を $-a$ と表す）.

(ii) 乗法について次の性質が成り立つ．
  (a) 任意の a, b, $c \in R$ について $(ab)c = a(bc)$.
  (b) 任意の a, $b \in R$ について $ab = ba$.
  (c)「任意の $a \in R$ について $1a = a$」という性質を持つ元 $1 \in R$ が存在する（**単位元**と呼ぶ）.

(iii) 加法と乗法について次の性質が成り立つ．
  (a) 任意の a, b, $c \in R$ について $(a+b)c = ac+bc$.

ついでに体の定義も与えておく．

定義. 可換環 R がさらに次の性質を持つとき，R は**体** (field) であるという．

(ii) 乗法について次の性質が成り立つ．
  (d) 0 でない任意の $a \in R$ に対して，$ab=1$ を満たす元 $b \in R$ が存在する（この b を a^{-1} と表す）.

(iv) $1 \neq 0$.

例 4.5. $\mathbb{Z}$ は当然可換環だし，$\mathbb{Z}/m\mathbb{Z}$ もそうである（問題 4.3）．さらに m が素数のとき $\mathbb{Z}/m\mathbb{Z}$ は体となる（問題 4.4）.

注 4.6. 可換環の定義において，(i) の (c) により存在が要請される元 $0 \in R$ は一意的である．なぜなら，$0_1, 0_2 \in R$ が両方ともここで述べられている性質を持つとすれば，$0_1+0_2=0_1$ であり，かつ (i) の (b) を合わせて用いれば $0_1+0_2=0_2$ でもあるから，$0_1=0_2$ となるからである．同様の一意性は他にもある（問題 4.2）.

注 4.7. (ii) の (b) が成り立たないだけで，可換環に要請される他の性質がすべて満たされている場合には，R は（単位元を持つ）**非可換環** (noncommutative ring) であるという．非可換環も重要だが（$n \geq 2$ のとき $n \times n$ 行列全体の集合が非可換環をなすことを考えれば，重要性は了解できるものと思う），話がややこしくなるので，ここでは扱わない．

定義の中で「加法と乗法と呼ばれる演算」という表現をしたが，これは線型空間（ベクトル空間）に対し

「加法とスカラー倍と呼ばれる演算」の存在を要請するのと同様である．「加法」や「乗法」の具体的な定義は，上記の諸性質を満たす限りにおいて，どのようなものを与えてもかまわない．

例 4.8 (多項式環). 体 K に対し（$\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ などを思い浮かべよう），K の元を係数とする X の多項式 (polynomial) 全体の集合を $K[X]$ で表す．多項式に対する通常の加法と乗法により，$K[X]$ は可換環をなす．これを K 上の（1 変数）**多項式環**と呼ぶ．

例 4.9 (形式的冪級数環). 体 K に対し，K の元を係数とする X の形式的冪級数全体の集合を $K[\![X]\!]$ で表す．ここで X の**形式的冪級数** (formal power series) とは

$$f(X) = a_0 + a_1X + a_2X^2 + a_3X^3 + \cdots = \sum_{n=0}^{\infty} a_nX^n, \qquad a_0, a_1, a_2, \ldots \in K$$

という“形式的な式”のことである．形式的冪級数 $f(X)$ は，その係数を並べて得られる列 $(a_n)_{n=0}^{\infty}$ と同一視される．形式的冪級数の加法および乗法は（無限個の項があるので一見すると明らかではないが）自然に定義される．つまり，$f(X)$, $g(X) \in K[\![X]\!]$ に対し，各々の係数を並べて得られる列を $(a_n)_{n=0}^{\infty}$, $(b_n)_{n=0}^{\infty}$ として，

$$c_n = a_n + b_n, \qquad d_n = \sum_{k=0}^{n} a_kb_{n-k}$$

とおき，$(c_n)_{n=0}^{\infty}$, $(d_n)_{n=0}^{\infty}$ に対応する形式的冪級数を，それぞれ和 $f(X) + g(X)$ および積 $f(X)g(X)$ と呼ぶ．こうして $K[\![X]\!]$ は可換環となるので，これを K 上の（1 変数）**形式的冪級数環**と呼ぶ．

例 4.10. 体 K に対し，各項が K の元であるような数列 $(a_n)_{n=1}^{\infty}$ 全体の集合を R とする．R において

$$(a_n)_{n=1}^{\infty} + (b_n)_{n=1}^{\infty} = (a_n + b_n)_{n=1}^{\infty}, \qquad (a_n)_{n=1}^{\infty}(b_n)_{n=1}^{\infty} = (a_nb_n)_{n=1}^{\infty}$$

と定めれば，R は可換環となる．記号 (c) によってすべての項が $c \in K$ に等しいような数列（定数列）を表すことにすれば，R の零元は定数列 (0)，単位元は定数列 (1) である．

次に，$\mathbb{Z}$ における部分集合 $m\mathbb{Z}$ と同じ役割を果たすものとして，可換環のイデアルの概念を定義する．

定義. R を可換環とする．R の部分集合 I であって

(i) $0 \in I$, (ii) $x, y \in I$ ならば $x + y \in I$, (iii) $x \in I$, $a \in R$ ならば $ax \in I$

という 3 つの条件を満たすもののことを，R の**イデアル**と呼ぶ．

一般に可換環 R とそのイデアル I が与えられたとき，R 上の同値関係 $\sim$ を

$$x \sim y \overset{\text{def}}{\Leftrightarrow} x - y \in I \tag{4.6}$$

によって定義することができる．この同値関係による同値類をイデアル I による**剰余類** (residue class) といい，$a \in R$ の属する剰余類を $[a]$ とか $a + I$ などと書く（後者は「$a + I$」全体で一つの記号である）．また，商集合 $R/\sim$ を R/I と書く．

すると次の定理で述べるように，$\mathbb{Z}/m\mathbb{Z}$ の場合とまったく同じようにして，R/I には加法と乗法が定義され，R/I は可換環となる．これを R のイデアル I による**剰余環** (residue class ring) または**商環** (quotient ring) と呼ぶ．

定理 4.11. 可換環 R とそのイデアル I に対し，同値関係 (4.6) による商集合 R/I を考える．すると，剰余類 $[a]$, $[b] \in R/I$ に対し

$$[a] + [b] = [a + b], \qquad [a][b] = [ab]$$

と定めることにより R/I にも加法と乗法を well-defined に定義することができ，R/I もまた可換環となる．

4.2 複素数の構成

ここまでで述べた一般論を適用することにより，実数体 $\mathbb{R}$ から複素数体 $\mathbb{C}$ を構成してみよう．

なお，今から述べる方法によらなくても，実数の対 $(a, b) \in \mathbb{R}^2$ を「$a + bi$」という複素数とみなす方法によって素朴に $\mathbb{C}$ を構成することもできる（問題 4.9）．だがここで説明する方法のほうが発展性がある．

●多項式環を用いた複素数体の構成

複素数体 $\mathbb{C}$ とは何だろうか.「$\mathbb{R}$ に新しい元 $i=\sqrt{-1}$ を“添加した”もの」というのが，ここで採用する説明である．ここで“添加する”と言っているのは，単に和集合 $\mathbb{R}\cup\{i\}$ を考えるということではなくて，i という元から（もともと $\mathbb{R}$ に属していた元たちも用いながら）生み出すことのできる“数”をすべて元として追加するということである．したがってたとえば，次のような“数”はすべて $\mathbb{C}$ の元となるわけだ.

$$i+5,\qquad 2i^2-\sqrt{3}\,i+5,\qquad i^2+1,\qquad \pi i^{100}-\sqrt{2}i^{20}-e.$$

これらは，言わば i の多項式の形をしている．実数を係数とする任意の多項式 $f(X)\in\mathbb{R}[X]$ に対し，X に i を代入した $f(i)$ はすべて $\mathbb{C}$ の元と考えられるべきであり，そのような $f(i)$ をすべて集めることにより $\mathbb{C}$ が得られるはずである.

ところで，すべての多項式 $f(X)$ が $\mathbb{C}$ の相異なる元を与えるということにはならない．われわれは i^2 を -1 と同一視する．言い換えれば，i^2+1 を 0 と同一視する．すなわち，X^2+1 という多項式は $0\in\mathbb{C}$ を与えるものと考えることになる．さらに，2 つの多項式 $f(X)$, $g(X)$ は，それらの差が X^2+1 で割り切れる多項式であるときに，同一の $\mathbb{C}$ の元を与える．ということは，多項式が $\mathbb{C}$ の元を与えるというよりもむしろ，

$$f(X)\sim g(X)\overset{\text{def}}{\Leftrightarrow} f(X)-g(X)=(X^2+1\text{ で割り切れる多項式}) \tag{4.7}$$

によって定義した同値関係 $\sim$ による同値類が $\mathbb{C}$ の元を与えると考えたほうが無駄がない.

ここで，さらに発想を一段階飛躍させる——そういった多項式の同値類そのものが $\mathbb{C}$ の元なのだと言うことが許されるのではないだろうか！ つまり，商集合 $\mathbb{R}[X]/\!\sim$ こそが $\mathbb{C}$ であると言い切ってしまえるのではなかろうか！ これが今から行う複素数体 $\mathbb{C}$ の定義のアイディアである.

定義を整った形で述べる前に，一つ注意をしておこう．(4.7) の同値関係の定義は，イデアルを用いて表すことができる．実際,

$$I=\{\,(X^2+1)q(X)\mid q(X)\in\mathbb{R}[X]\,\} \tag{4.8}$$

と定めれば, これは多項式環 $\mathbb{R}[X]$ のイデアルになっている．そして (4.7) は $f(X)\sim g(X)$ を $f(X)-g(X)\in I$ によって定義するということに他ならない.

定義. 実数体 $\mathbb{R}$ 上の多項式環 $\mathbb{R}[X]$ の，式 (4.8) によって与えられるイデアル I による剰余環 $\mathbb{R}[X]/I$ のことを $\mathbb{C}$ と書き，その元のことを**複素数** (complex number) という．実数 $a\in\mathbb{R}$ は，a を定数項のみを持つ多項式と考え，剰余類 $[a]\in\mathbb{R}[X]/I=\mathbb{C}$ に対応づけることによって，複素数と見なされる．また，X という多項式が定める複素数 $[X]\in\mathbb{R}[X]/I=\mathbb{C}$ のことを i と書く.

この定義に慣れる目的も兼ねて，複素数についてよく知っている性質のうち 2 つを証明してみよう.

命題 4.12. 任意の複素数 $\alpha\in\mathbb{C}$ は，ある実数 $a,b\in\mathbb{R}$ によって $\alpha=a+bi$ と表される.

［証明］ 任意の $\alpha\in\mathbb{C}$ は，ある多項式 $f(X)\in\mathbb{R}[X]$ によって $\alpha=[f(X)]$ と表すことができる．ここで $f(X)$ を X^2+1 で割った商を $q(X)$，余りを $r(X)$ とする：

$$f(X)=(X^2+1)q(X)+r(X).$$

$(X^2+1)q(X)$ はイデアル I に属するので，$f(X)\sim r(X)$，すなわち $\alpha=[f(X)]=[r(X)]$ である．ところで X^2+1 は 2 次式なので，余り $r(X)$ は高々 1 次式．そこで $r(X)=a+bX$ $(a,b\in\mathbb{R})$ と表すことができ，$\alpha=[r(X)]=[a+bX]=[a]+[b][X]=a+bi$ である． □

定理 4.13. $\mathbb{C}$ は体である.

［証明］ 多項式としての 1 と 0 の差 $1-0=1$ がイデアル I に属していないことから，$\mathbb{C}=\mathbb{R}[X]/I$ の零元と単位元は異なる．あとは 0 でない任意の $\mathbb{C}$ の元が逆元を持つことを証明すればよい.

α を 0 でない $\mathbb{C}$ の元とする．命題 4.12 により $\alpha = a + bi$ $(a, b \in \mathbb{R})$ と表すことができる．ここで $\alpha \neq 0$ だから，a, b の少なくとも一方は 0 ではなく，よって $a^2 + b^2 \neq 0$ である．そこで

$$\beta = \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2} i$$

とおけば $\alpha\beta = 1$ である． □

これで $\mathbb{C}$ を**複素数体** (the field of complex numbers) と呼ぶことができるようになった．

演習問題

4.1　命題 4.3 において，条件 (iv) は (4.5b) が成立するために必要でもあることを証明せよ．

4.2　可換環および体の定義に関して次のことを証明せよ．

(1)　「任意の $a \in R$ について $1a = a$」という性質を持つ元 $1 \in R$ は一意的である．

(2)　任意の $a \in R$ に対し，$a + b = 0$ を満たす元 $b \in R$ は一意的である．

(3)　0 でない任意の $a \in R$ に対し，$ab = 1$ を満たす元 $b \in R$ は一意的である．

4.3　例 4.5 で触れたように $\mathbb{Z}/m\mathbb{Z}$ は可換環であるが，その零元は何か．単位元は何か．またそれらが実際に零元，単位元であることを直接確かめよ．

4.4　正整数 m に対し，$\mathbb{Z}/m\mathbb{Z}$ が体であるための必要十分条件は，m が素数であることである．そのことを示せ．（ヒント：p を素数，n を p の倍数でない整数とするとき，Euclid の互除法によって $ap + bn = 1$ となるような $a, b \in \mathbb{Z}$ が存在することがわかる．）

4.5　集合 X に対し，その冪集合 $\mathscr{P}(X)$ を考える．X の部分集合 A, B に対し $A+B = (A \setminus B) \cup (B \setminus A)$, $AB = A \cap B$ によって和 $A + B$ と積 AB を定めれば，これらの演算により $\mathscr{P}(X)$ は可換環になることを証明せよ（集合 X の定める **Boole 環**．なお，$(A \setminus B) \cup (B \setminus A)$ は A と B の**対称差**と呼ばれる）．

4.6　$\mathbb{Z}$ のイデアル I は，必ずある整数 m によって $I = m\mathbb{Z}$ と表されることを証明せよ．（$m = 0$ も許していることに注意.）（ヒント：$I \neq \{0\}$ のとき，$I \cap \{1, 2, 3, \dots\}$ の最小元を m とおく．）

4.7

(1)　一般に，可換環 R のイデアル I, J に対し，$I + J = \{a + b \mid a \in I, b \in J\}$ および $I \cap J$ も R のイデアルであることを証明せよ．

(2)　$R = \mathbb{Z}$ について考える．正整数 m, n に対し，それらの最大公約数を d，最小公倍数を l とすれば $m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$, $m\mathbb{Z} \cap n\mathbb{Z} = l\mathbb{Z}$ であることを証明せよ．

4.8　$\mathbb{R}$ 上の形式的冪級数環 $\mathbb{R}[\![X]\!]$ において，$f(X) = 1 - X$ には逆元すなわち $f(X)g(X) = 1$ となるような $g(X) \in \mathbb{R}[\![X]\!]$ が存在する．その逆元を具体的に与えよ．

4.9　$\mathbb{R}^2$ に次のように加法と乗法を導入する．

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2), \qquad (a_1, b_1)(a_2, b_2) = (a_1a_2 - b_1b_2, a_1b_2 + a_2b_1).$$

これらの演算に関して $\mathbb{R}^2$ は可換環となる（確かめなくてよい）．写像 $\Phi\colon \mathbb{R}^2 \to \mathbb{C}$ （ここでは本文で説明したとおり $\mathbb{C} = \mathbb{R}[X]/I$ と考えている）を $\Phi((a, b)) = [a + bX]$ によって定義する．次を証明せよ（このことを指して，Φ は $\mathbb{R}^2$ から $\mathbb{C}$ への**環の同型写像**であるという）．

(1)　$\Phi\colon \mathbb{R}^2 \to \mathbb{C}$ は全単射である．

(2)　$\Phi((a_1, b_1) + (a_2, b_2)) = \Phi((a_1, b_1)) + \Phi((a_2, b_2))$, $\Phi((a_1, b_1)(a_2, b_2)) = \Phi((a_1, b_1))\Phi((a_2, b_2))$.

4.10　$\mathbb{R}$ の部分集合 $R = \{m + n\sqrt{2} \mid m, n \in \mathbb{Z}\}$ を考える．これは実数の通常の加法，乗法によって可換環となるが，体にはなっていない．$\alpha = m + n\sqrt{2} \in R$ が R において逆元を持つための必要十分条件が $m^2 - 2n^2 = \pm 1$ で与えられることを証明せよ．