2012 年度 後期 代数学 2

更新日時 2013-01-24 20:27:41　担当 和地 輝仁

目 次

末尾の演習問題を、今年度用に調整しました。みなさん頑張って勉強して下さい。

1　シラバス抜粋

到達目標

1. 分数の性質を知る。
2. 無限小数の性質を知る。
3. 環とその性質を知る。
4. 多項式の既約性の判定法を理解する。

授業計画　順序を交換する場合もあるので注意すること。

1. 合同式
2. 分数と小数
3. 循環小数
4. 純循環小数
5. 混循環小数
6. オイラーの関数
7. 循環節の性質
8. 環
9. 環の性質
10. 整域
11. イデアル
12. 単項イデアル整域
13. 多項式環
14. 多項式の既約性
15. 期末試験

成績評価　期末試験 (80%) と、毎回の演習問題の状況 (20%) で成績を評価する。原則として全ての時間の出席を求めるが、やむを得ない理由で欠席をする (した) 場合はできるだけ速やかに申し出て、指示を受けること。

2 授業のノート

§1 合同式

(1.1) **合同** 整数 a, b と整数 m に対し、$a-b$ が m の倍数であるとき、a と b は m を法として**合同**であると言い、$\boldsymbol{a \equiv b \pmod{m}}$ と書く。

(1.2) **同値関係** 合同の関係は、次を満たす。

(E1) $a \equiv a \pmod{m}$ (対称律)
(E2) $a \equiv b \pmod{m}$ ならば $b \equiv a \pmod{m}$ (反射律)
(E3) $a \equiv b \pmod{m}$ かつ $b \equiv c \pmod{m}$ ならば $a \equiv c \pmod{m}$ (推移律)

(1.3) **補題** 整数 a, b, c, d と整数 m に対して、$a \equiv b \pmod{m}$, $c \equiv d \pmod{m}$ とするとき次が成り立つ。

(1) $a + c \equiv b + d \pmod{m}$
(2) $a - c \equiv b - d \pmod{m}$
(3) $ac \equiv bd \pmod{m}$

(1.4) **例** $9 + 12 \equiv 4 + 2 \equiv 6 \equiv 1 \pmod{5}$.

(1.5) **問題** 次の問に答えよ。

(1) $221 \times 329 \pmod{11}$ を簡単にせよ。
(2) $22^{22} \pmod{5}$ を簡単にせよ。
(3) 23^{23} を 7 で割った余りを求めよ。
(4) $x^3 + x^2 \equiv \pmod{3}$ を満たす x $(x = 0, 1, 2)$ をすべて求めよ。
(5) $x^3 + x^2 \equiv \pmod{6}$ を満たす x $(x = 0, 1, \ldots, 5)$ をすべて求めよ。

(1.6) **例 (n の倍数であることの判定法)**

(1) 正の整数の各位の数を加えて 3 の倍数になれば、元の整数も 3 の倍数である。
(2) 正の整数の各位の数を加えて 9 の倍数になれば、元の整数も 9 の倍数である。
(3) 正の整数の各位の数の交代和 (符号を交互に変えた和) が 11 の倍数になれば、元の整数も 11 の倍数である。

(1.7) **問題** 次の問に答えよ。

(1) n を非負整数とするとき、$3^{n+2} + 4^{2n+1}$ が 13 の倍数であることを示せ。
(2) n を非負整数とするとき、$3^{4n+1} + 4^{n+1}$ が 7 の倍数であることを示せ。

(1.8) **ユークリッドの互除法** 正整数 a, b に対して、a を b で割った余りを r とすると、$(a, b) = (r, b)$ である。この関係を用いて数を小さくしていき最大公約数を求めるアルゴリズムを**ユークリッドの互除法**と呼ぶ。

(1.9) **ベズーの等式** 整数 a, b が互いに素ならば、

$$ax + by = 1$$

を満たす整数 x, y が存在する。

(1.10) **問題** 次の方程式を満たす整数解を 1 組求めよ。

(1) $96x + 29y = 1$
(2) $96x - 29y = 1$
(3) $35x + 13y = 1$
(4) $35x + 13y = 2$

(1.11) **問題** 次の方程式を満たす整数 x を 1 つ求めよ。

(1) $96x \equiv 1 \pmod{29}$
(2) $13x \equiv 1 \pmod{35}$
(3) $35x \equiv 2 \pmod{13}$

(1.12) **定義 (有理整数環の剰余環)** (0 ではない整数) m に対して、m を法とした合同の関係について、$\mathbb{Z}$ の**剰余集合**を考える。つまり、次で定まる **剰余類**

$$\overline{a} = \{x \in \mathbb{Z} \mid x \equiv a \pmod{m}\}$$

のなす集合

$$\{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$$

を考え、これを $\mathbb{Z}/(\boldsymbol{m})$ と書く。(1.3) より、$\mathbb{Z}/(m)$ に次の演算が定まる。

$$\overline{a} + \overline{b} = \overline{a+b}, \qquad \overline{a} - \overline{b} = \overline{a-b}, \qquad \overline{a}\overline{b} = \overline{ab}$$

(1.13) **補題 ($\mathbb{Z}$ の剰余環の元が逆元を持つための必要十分条件)** a, m を整数とする。$\mathbb{Z}/(m)$ において、$\overline{a}$ の逆元が存在するための必要十分条件は $(a, m) = 1$ となることである。

(1.14) **問題 (剰余環における逆元)** $\mathbb{Z}/(13)$ において、$\overline{5}$, $\overline{7}$, $\overline{9}$ の逆元を求めよ。

(1.15) **定義 (オイラーの関数)** 正の整数 n に対して、1 から n までの整数のうち n と互いに素なものの個数を、$\boldsymbol{\phi(n)}$ で書く。この ϕ を**オイラーの関数**と呼ぶ。

(1.16) **命題 (オイラーの関数の性質)**

(1) 素数 p に対して、$\phi(p) = p - 1$.
(2) 素数 p と正整数 n に対して、$\phi(p^n) = p^n - p^{n-1}$.
(3) 互いに素な正整数 m, n に対して、$\phi(mn) = \phi(m)\phi(n)$.

Proof. (1) 明らか。

(2) p^n と互いに素とは p と互いに素ということだから、1 から p^n のうち、p の倍数が p^n/p 個あることよりわかる。

(3) $km+ln = 1$ とできる。$(k, n) = (m, l) = 1$ にも注意しておく。$bkm+aln$ $(0 \le a < m, 0 \le b < n)$ は mn を法としてすべて異なる。これらを mn で割った余りはすべて異なるから、ちょうど 0 から $mn-1$ までであり、この余りのうち mn と互いに素であるものを数えたい。しかし、mn と互いに素かどうかは、余りをとっても変わらないから、$bkm+aln$ のまま考えてよい。$(a, m) > 1$ または $(b, n) > 1$ ならば、$(bkm + aln, mn) > 1$ である。逆に、$(a, m) = 1$ かつ $(b, n) = 1$ ならば、$(bkm + aln, m) = 1$ かつ $(bkm + aln, n) = 1$ だから、$(bkm + aln, mn) = 1$ である。よって、mn と互いに素である (a, b) の総数は、$\phi(m)\phi(n)$ 個である。 □

(1.17) **オイラーの定理** 互いに素な正の整数 a, n に対して次の合同式が成立する。

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

(1.18) **補題 (指数)** 互いに素な正の整数 a, n に対して合同式

$$a^e \equiv 1 \pmod{n}.$$

が成立するような最小の正整数 e は、オイラーの関数 $\phi(n)$ の約数である。

(1.19) **フェルマーの小定理** 素数 p と整数 a に対して、$a^p \equiv a \pmod{p}$.

(1.20) **問題** 次の整数を、指定された法に関して合同な、最小の正整数にせよ。

(1) $5^{22} \pmod{19}$
(2) $19^{17} \pmod{17}$
(3) $22^{23} \pmod{17}$
(4) $5^{16} \pmod{48}$
(5) $7^{18} \pmod{60}$

(1.21) **ウィルソンの定理** 素数 p に対して、$(p-1)! \equiv -1 \pmod{p}$.

(1.22) **ウィルソンの定理の逆** 1 より大きい整数 m に対して、$(m-1)! \equiv -1 \pmod{m}$ ならば、m は素数である。

§2 分数と小数

(2.1) **定義 (10 進表記)** 0 から 9 までの数字たち $a_n, a_{n-1}, \ldots, a_1, a_0$ と $b_1, b_2, b_3, \ldots$ が与えられたとする。a_n は 0 と異なるとする。このとき、**10 進表記**

$$a_n a_{n-1} \cdots a_1 a_0 \,.\, b_1 b_2 b_3 \cdots$$

の値を、

$$\begin{aligned} &10^n a_n + \cdots + 10^1 a_1 + 10^0 a_0 + \frac{b_1}{10^1} + \frac{b_2}{10^2} + \cdots \\ &\quad = \lim_{m\to\infty} (10^n a_n + \cdots + 10^1 a_1 + 10^0 a_0 + \frac{b_1}{10^1} + \frac{b_2}{10^2} + \cdots + \frac{b_m}{10^m}) \end{aligned}$$

で定める。

※ これは収束する (連続の公理と、小数部分が m によらず 1 を超えないので上界が存在することによる)

※ 1 つの表記に対して 1 つの実数が定まるのであり、1 つの実数に対して 1 つの表記が定まるというわけではない。つまり、1 という実数に対して「1」と「$0.999\cdots$」という 2 つの表記があることは、何の矛盾も引き起こさない。

(2.2) **事実 (絶対収束級数の項の順序交換)** 無限級数 (無限数列の和)

$$C = c_1 + c_2 + \cdots + c_n + \cdots = \lim_{n\to\infty} (c_1 + c_2 + \cdots + c_n)$$

が**絶対収束**するとは、各項を絶対値をとった無限級数

$$|c_1| + |c_2| + \cdots + |c_n| + \cdots$$

が収束することを言う。絶対収束する無限級数は収束する。

2 つの絶対収束する無限級数

$$C = c_1 + c_2 + \cdots, \qquad D = d_1 + d_2 + \cdots$$

に対して、和 $C + D$ や 差 $C - D$ において項の順序を任意に入れ替えても結果は変わらない。この事実を認めると、

```
   9.999999...
-) 0.999999...
---------------
   9
```

のような筆算は正しい計算であることがわかる。

(2.3) **問題** 次の循環小数を既約分数に直せ。

(1) $0.1\dot{2}\dot{3} = 0.1232323\cdots$
(2) $1.2\dot{3}4\dot{5} = 1.2345345\cdots$

分数が有限小数あるいは循環小数になるための必要十分条件を与えよう。

(2.4) **命題 (有限小数になるための必要十分条件)** 互いに素な正の整数 m, n に対して、既約分数 m/n を考える。

(1) $n = 2^a 5^b$ (a, b は非負整数) の形ならば、m/n は有限小数である。
(2) そうでないならば、m/n は循環小数である。

Proof. (1) 分母を $10^{\max(a,b)}$ にできるから有限小数である.
(2) 有限小数は, 分母が 10^e の形の分数で書ける. 既約分数 m/n の分母に 2 と 5 以外の素因数があれば, 分子・分母を何倍しても分母を 10^e の形にはできないから, m/n は無限小数である.
また, 実際に割り算を実行すると割り切れないので, その余りは $1, 2, \ldots, n-1$ の $n-1$ 通りしかない. したがって (割り算の商が小数部分に入ってから), 高々 $n-1$ 回目で同じ余りが出現して, その先は同じ割り算の反復になる. よって, m/n は循環小数になる. □

(2.5) **注意 (循環小数と進法)** 有限小数になるかどうかは、上で見たように進法に関係している。例えば、有限 2 進小数になる既約分数は、分母が 2^e の形の場合に限る。

(2.6) **定義 (循環節)** 循環小数の、循環する部分のことを**循環節**と呼ぶ。循環節の長さがどう決まるかは以下で与えられる。

(2.7) **命題 (循環節の長さ)** 10 と互いに素な正整数 n に対して、$10^e \equiv 1 \pmod{n}$ を満たす最小の正整数を e とする (その存在は (1.17)、性質は (1.18))。このとき、既約な真分数 m/n (つまり m, n は互いに素で、$1 \le m \le n-1$) は循環節の長さが e である循環小数であり、循環は小数第 1 位から始まる。

※ 既約でなければ、$1/21 = 0.0\dot{4}7619\dot{0}$ と $7/21 = 0.\dot{3}$ のように循環節の長さは異なるかも知れない。

Proof. $10^e \equiv 1 \pmod{n}$ より、$10^e = na + 1$ と書ける (a は整数)。すると、

$$\begin{aligned}\frac{m}{n} = \frac{ma}{na} &= \frac{ma}{10^e - 1} \\ &= \frac{ma \cdot 10^{-e}}{1 - 10^{-e}} \qquad \leftarrow \text{(等比級数の和の形をしている)} \\ &= ma \cdot 10^{-e} + ma \cdot 10^{-2e} + ma \cdot 10^{-3e} + \cdots \\ &= \frac{ma}{10^e} + \frac{ma}{10^{2e}} + \frac{ma}{10^{3e}} + \cdots .\end{aligned}$$

ここで、$m < n$ より、$ma < na = 10^e - 1$ だから ma は高々 e 桁の整数である。よって、m/n は e 桁ごとに同じ数字の来る小数に展開される。また、循環が小数第 1 位から始まることもわかる。

しかし、$ma = 123123$ のように ma 自体が循環していると、循環節の長さは e より短かくなるため、そうならないことを言う必要がある。

仮に循環節の長さが e' ($e' < e$) であったとすると、$m/n = m' \cdot 10^{-e} + m' \cdot 10^{-2e} + m' \cdot 10^{-3e} + \cdots$ と書けるから、$m/n = m'/(1 - 10^{e'})$ となる。m と n は互いに素だから、整数 a を用いて、$ma = m'$、$na = 1 - 10^{e'}$ と書け、$10^{e'} \equiv 1 \pmod{n}$ となる。これは e の最小性に反するから、循環節の長さは e である。 □

(2.8) **系 (循環節の長さとオイラーの関数)** 10 と互いに素な正整数 n と、$1 \le m \le n-1$ なる整数 m があるとき、m/n を循環小数にしたときの循環節の長さは、オイラーの関数 $\phi(n)$ の約数である。

(2.9) **例 (循環節の長さ)** 次の例では、循環節の長さがオイラーの関数の約数になっていることが確認できる。

(1) 分数 1/7 を考える。$1/7 = 0.\dot{1}42857\dot{}$ であり、循環節の長さは 6 である。オイラーの関数は $\phi(7) = 6$ である。
(2) 分数 11/21 を考える。$11/21 = 0.\dot{5}23809\dot{}$ であり、循環節の長さは 6 である。また、オイラーの関数は $\phi(21) = 12$ である。
(3) 分数 10/13 を考える。$10/13 = 0.\dot{7}6923\dot{0}$ であり、循環節の長さは 6 である。また、オイラーの関数は $\phi(13) = 12$ である。

(2.10) **定義 (純循環小数、混循環小数)** 循環小数が**純循環小数**であるとは, 例えば $0.123123\cdots$ のように, 循環節が小数第 1 位から始まることを言う. 逆に, 例えば $0.99123123\cdots$ のように, 循環節が小数第 1 位よりも後ろから始まる循環小数を**混循環小数**と言う.

(2.11) **定理 (有限、純循環、混循環小数になるための必要十分条件)** 互いに素な正整数 m, n $(m < n)$ に対して既約分数 m/n を考えるとき、次が成立する。

(1) $n = 2^a 5^b$ と書けるとき m/n は有限小数である。このとき、$c = \max\{a, b\}$ とすると、m/n は小数第 c 位まである。
(2) n の素因数分解に 2 も 5 も現れないとき、m/n は純循環小数である。このとき、$10^e \equiv 1 \pmod{n}$ を満たす最小の正整数を e とすると、循環節の長さは e である。
(3) それ以外の場合、つまり, n の素因数分解に 2 か 5 の一方または両方が現れ、かつ、2 でも 5 でもない素数も現れるとき、m/n は混循環小数である。このとき、$n = 2^a 5^b n'$ (n' の素因数分解には 2 も 5 も現れない) と書き、$c = \max\{a, b\}$ とおき、$10^e \equiv 1 \pmod{n'}$ を満たす最小の正整数を e とおくと、m/n の循環節は小数第 $(c+1)$ 位から始まり、その長さは e である。

(2.12) **例 (有限、純循環、混循環小数)** (1) 既約分数 34567/125000 は、分母が $2^3 5^6$ だから有限小数であり、$\max\{3, 6\} = 6$ なので小数第 6 位まである。実際に割り算してみると、0.276536 である。

(2) 既約分数 11/21 は、分母の素因数分解 $3 \cdot 7$ に 2 も 5 も現れないので純循環小数である。また、$10^e \equiv 1 \pmod{21}$ を満たす最小の e は 6 であるから (循環節も求めるのであれば、1/21 の割り算を実行して $e = 6$ を求めるのが結局は速い)、循環節の長さは 6 である。実際に割り算してみると、$0.\dot{5}23809\dot{}$ である。

(3) 既約分数 1237/1750 は、分母の素因数分解が $2^1 5^3 7^1$ であるから、混循環小数である。$\max\{1, 3\} = 3$ だから、循環節は小数第 4 位から始まる。また、循環節の長さは、1/7 の場合と同じであるから 6 である。実際に割り算してみると、$0.706\dot{8}57142\dot{}$ である。

(2.13) **問題 (有限、純循環、混循環小数になる分数を求める)**

(1) 小数第 5 位まである有限小数になるような分数を 1 つ答えよ。
(2) 純循環小数になるような分数を 1 つ答えよ。
(3) 小数第 4 位から循環節が始まるような混循環小数になるような分数を 1 つ答えよ。

§3 循環節の性質

さて、$1/7 = 0.\dot{1}42857\dot{}$ の循環節 142857 を 142 と 857 に分けて足すと、$142 + 857 = 999$ となり、$2/7 = 0.\dot{2}85714\dot{}$ でも同様に $285 + 714 = 999$ となる。また、$3/17 = 0.\dot{1}764705882352941\dot{}$ でも同様に、$17647058 + 82352941 = 99999999$ である。しかし、$11/21 = 0.\dot{5}23809\dot{}$ では、$523 + 809 = 1332$ となってしまう。このような違いが何によっておこるのかがわかる。

(3.1) **命題 (循環節を半分に切断して加えると $99\cdots9$)** 正整数 n が 10 と互いに素のとき、既約真分数 m/n は純循環小数であった。その循環節の長さ e が偶数であるとする。$10^{e/2} \equiv -1 \pmod{n}$ ならば、循環節を中央で 2 等分して、それぞれを $e/2$ 桁の整数と見なして加えると $99\cdots9$ ($e/2$ 桁の整数) になる。

Proof. $10^k m$ を n で割ったときの余りを r とすると、$m \div n$ を実行して小数第 k 位に商が立ったときの余りは r に等しいことに注意しておく。

$$10^{k+e/2} m \equiv -10^k m \equiv -r \equiv n - r \pmod{n}$$

だから、$10^{k+e/2} m$ を n で割った余りは $n - r$ である。

r あるいは $n-r$ が余りに出た次の割り算を考えると、割られる数は $10r$ や $10(n-r)$ になる。$10r$ を n で割った商を q とすると、$10r = nq+s$ $(1 \leq s < n)$ であるから、

$$10(n-r) = 10n - 10r = 10n - nq - s = (9-q)n + (n-s)$$

となり、$10(n-r)$ を n で割った商は $9-q$ である。したがって、k 番目の商と $k+e/2$ 番目の商は加えると 9 になる。 □

(3.2) **例 (循環節の切断)** (1) 2/7 の場合, 下の割り算で 3 回目の余りに 5 ($\equiv -2 \pmod 7$) が現れた時点で, その後の 3 つの商は, $999-285=142$ と求めてよい. また, 余りに着目すると, (最初の割られる数 2 も付け足して) はじめの 3 つは, 2, 6, 4 であり, 残りの 3 つはこれらの -1 倍が, $5 \equiv -2 \pmod 7$, $1 \equiv -6 \pmod 7$, $3 \equiv -4 \pmod 7$ と続いている.

```
 0.2 8 5 7 1 4 2 ...
---------------
7)2
  1 4
  ---
    6 0
    5 6
    ---
      4 0
      3 5
      ---
        5 0
        4 9
        ---
          1 0
            7
          ---
            3 0
            2 8
            ---
              2 0
              1 4
              ---
                6 0 ...
```

(2) 11/21 の場合, 下の割り算の途中で 10 ($\equiv -11 \pmod{21}$) という余りが出ないので, その後の商や余りがどうなるかはわからない.

```
   0.5 2 3 8 0 9 ...
---------------
2 1)1 1 0
    1 0 5
    -----
```

```
5 0
4 2
---
 8 0
 6 3
 ---
 1 7 0
 1 6 8
 -----
   2 0
     0
   ---
   2 0 0
   1 8 9
   -----
     1 1  ...
```

さて, 分母が 7 の場合, $1/7 = 0.\dot{1}42857\dot{}$, $2/7 = 0.\dot{2}85714\dot{}$, $3/7 = 0.\dot{4}28571\dot{}$ のように, すべての既約分数において, 循環節は 142857 をローテーションしたものになっている. しかし, 分母が 13 の場合, $1/13 = 0.\dot{0}76923\dot{}$, $2/13 = 0.\dot{1}53846\dot{}$ と 2 種類の循環節が現れる (分母が 3 の場合でも 2 種類の循環節が現れているので, 驚くほどのことではない). さらに, 分母が 27 の場合, $1/27 = 0.\dot{0}3\dot{7}$, $2/27 = 0.\dot{0}7\dot{4}$, $4/27 = 0.\dot{1}4\dot{8}$, のように, (既約分数ならば) 全部で 6 種類の循環節が現れる. このような違いは何によって起こるかが次でわかる.

(3.3) **命題 (循環節の「種類」)** 循環小数になるような分母 n を固定し, 既約分数 m/n の循環節の長さを e とする. このとき, 既約分数 m/n に現れうる循環節の「種類」は, $\phi(n)/e$ 個である. ただし, $\phi(n)$ はオイラーの関数であり, 循環節の「種類」とは, ローテーションして同じになる循環節を同じ「種類」と見なすことである.

(3.4) **例 (循環節の「種類」)** (1) 分母が 7 の場合, 循環節の長さは 6 であり, オイラーの関数の値も $\phi(7) = 6$ である. よって, 循環節の種類は $6/6 = 1$ 個である.

(2) 分母が 13 の場合, 循環節の長さは 6 であり, オイラーの関数の値は $\phi(13) = 12$ である. よって, 循環節の種類は $12/6 = 2$ 個である.

このとき, 例えば $1/13 = 0.\dot{0}76923\dot{}$ の循環節をローテーションした循環節を持つのは, どんな m に対する $m/13$ なのかは次にようにしてわかる. 1/13

の循環節を左に 1 つローテーションしてできる $0.\dot{7}69230\dot{}$ は, $1/13$ を 10 倍したものであるから, $10/13$ である. もう 1 回左にローテーションすると $100/13 = 7 + 9/13$ であるから, $9/13 = 0.\dot{6}92307\dot{}$ である. 同様にして続けると,

$$\begin{aligned} &1, \\ &10, \\ &10^2 \equiv 9 \pmod{13}, \\ &10^3 \equiv 12 \pmod{13}, \\ &10^4 \equiv 3 \pmod{13}, \\ &10^5 \equiv 4 \pmod{13} \end{aligned}$$

が分子のとき, 同じ種類の循環節を持つ.

ここに現れなかった 2, 5, 6, 7, 8, 11 は, もう 1 種類の循環節を持つ.

§4 環

(4.1) **定義 (環、可換環)** 2 種類の演算、和と積が定義された集合 R が **環** であるとは、次の条件 (R1) から (R7) を満たすときを言う。

(R1) 和が結合法則を満たす
(R2) 和が交換法則を満たす
(R3) 和の単位元 0 が存在する $(a + 0 = 0 + a = a)$
(R4) 和の逆元が存在する $(a + (-a) = 0$ なる $-a$ の存在$)$
(R5) 積が結合法則を満たす
(R6) 0 とは異なる積の単位元 1 が存在する $(a \cdot 1 = 1 \cdot a = a)$
(R7) 分配法則が成立する $(a(b + c) = ab + ac,\ (a + b)c = ac + bc)$

さらに、

(R8) 積が交換法則を満たす

も成立しているとき、R を **可換環** と呼ぶ。

可換環ではない環にも、$n \times n$ 行列全体のなす環 n **次全行列環** など重要なものがあるが、この講義では可換環のみを学ぶ。

(4.2) **例 (数のなす環)** 環の定義は条件が多く思えるかも知れないが、数の集合であれば、単に **1 と 0 を含み、和、差、積で閉じている集合** は環である、ということである。

(1) まず、複素数全体の集合 $\mathbb{C}$、実数全体の集合 $\mathbb{R}$、有理数全体の集合 $\mathbb{Q}$、整数全体の集合 $\mathbb{Z}$ はすべて環である。
(2) 偶数全体の集合 $2\mathbb{Z}$ は、1 を含まないので環ではない。ただし、それ以外の条件は満たしている。
(3) $\{a + b\sqrt{2}\,;\ a,b$ は整数 $\}$ は環である。
(4) m を法とした $\mathbb{Z}$ の剰余環 $\mathbb{Z}/(m)$ は (その名どおり) 環である。

(4.3) **定義 (単元、零因子、整域)** 環 R において、

(1) $a \in R$ が乗法の逆元を持つとき、a を **単元** という。ここに、a の逆元とは、$ab = 1$ を満たす $b \in R$ である。
(2) 0 ではない $b \in R$ に対して $ab = 0$ となるような $a \in R$ を R の **零因子** という。特に 0 は常に零因子である。
(3) 0 以外の零因子を持たない環を **整域** という。

(4.4) **補題 (単元は零因子ではない)** 環 R において、単元は零因子ではない。

(4.5) **例 (単元、零因子、整域)**

(1) 環 $\mathbb{Z}$ の単元は 1 と -1 のみである。
(2) 環 $\mathbb{Z}/(3)$ の単元は $\overline{1}$ と $\overline{2}$ である。したがって、環 $\mathbb{Z}/(3)$ は整域である。
(3) 環 $\mathbb{Z}/(4)$ において、$\overline{1}$ と $\overline{3}$ は単元であり、$\overline{2}$ は零因子である。
(4) $\mathbb{Z}$ は整域である。

(4.6) **定義 (体)** 0 以外のすべての元が単元であるような環を**体**と呼ぶ。例えば実数全体の集合 $\mathbb{R}$ は体である。また、(4.4) より、体は整域である。

(4.7) **命題 ($\mathbb{Z}/(m)$ が体であるための必要十分条件)** 2 以上の整数 m に対して、$\mathbb{Z}/(m)$ 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。

(4.8) **問題 ($\mathbb{Z}/(m)$ の零因子、逆元)**

(1) $\mathbb{Z}/(18)$ の零因子をすべて書け。
(2) それ以外の元は単元であるが、それらの逆元をそれぞれ求めよ (既習)。

(4.9) **問題 (標数)** 例えば体 $\mathbb{Z}/(p)$ では、1 を繰り返し加えていくと p 回目で始めて 0 になる。このように $m \cdot 1 = 0$ となる最小の m を体の**標数**と言う。また、実数体 $\mathbb{R}$ のように 1 を何回加えても 0 にならない場合は、標数は 0 と定める。体の標数が 0 でないならば、素数であることを示せ。

(4.10) **定義 (多項式環)** 環 R の元を係数に持つような X の多項式全体の集合を

$$R[X] = \left\{ a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 \, ; \quad \begin{array}{l} n \geq 0, \\ a_0, \ldots, a_n \in R \end{array} \right\}$$

で表し、R 上の **1 変数多項式環**と呼ぶ。また、$f \in R[X]$ の**次数**を $\deg f$ で表す。

例えば、$\mathbb{Z}$ を係数に持つ 1 次多項式は、$X+1, X+2, \ldots$ と無数にあるが、$\mathbb{Z}/(2)$ を係数に持つ 1 次多項式は、X と $X+\overline{1}$ の 2 つしかない。2 次でも 4 つしかなく、このことを用いれば、$X^2+X+\overline{1}$ や $X^3+X+\overline{1}$ の既約性などもわかってしまう。

(4.11) **割り算の恒等式** R を環、$f, g \in R[X]$ とする。g の最高次係数が単元 (例えば 1) のとき、

$$f = qg + r \qquad (q, r \in R[X],\ \deg r < \deg g)$$

と一意的に書ける。

(4.12) **定理 (剰余の定理、因数定理)** 環 R 上の多項式 $f \in R[X]$ と、$a \in R$ に対して、

(1) f を $X-a$ で割った余りは、$f(a)$ に等しい。
(2) f が $X-a$ $(a \in R)$ で割り切れるための必要十分条件は $f(a) = 0$ となることである。

※ $f(a) = 0$ となることを a は f の**根**であると言う。

(4.13) **定理 (根の個数の上限)** 整域 R 上の n 次多項式の異なる根の個数は n 以下である。

(4.14) **例 (係数環が整域ではない多項式の根の個数)** $\mathbb{Z}/(6)$ は整域ではない。2 次多項式 $X^2 - X$ は $X = \overline{0}, \overline{1}, \overline{3}, \overline{4}$ の 4 つの根を持つ。

§5 多項式の既約性

(5.1) **定義** 環 R 上の多項式環 $R[X]$ の多項式 $f \in R[X]$ が**可約**であるとは、f よりも次数の低い 2 つの多項式 $g, h \in R[X]$ によって $f = gh$ と書けることを言う。$f \in R[X]$ が**既約**であるとは、可約ではないことを言う。

(5.2) **命題** 整数係数の多項式 $f \in \mathbb{Z}[X]$ が既約ならば、係数を有理数まで広げて $\mathbb{Q}[X]$ の中で考えても既約である。

(5.3) **命題** $f \in \mathbb{Z}[X]$ と、素数 p に対して、係数をすべて $K = \mathbb{Z}/(p)$ で考えた多項式を $\overline{f} \in K[X]$ と書くことにする。$\mathbb{Z}[X]$ の中で $f = gh$ ならば、$K[X]$ の中で、$\overline{f} = \overline{g}\overline{h}$ である。

特に、f の最高次係数が p の倍数でなく、$\overline{f}$ が $K[X]$ で既約ならば、f も既約である。

(5.4) **例** 次の整数係数多項式は有理数係数の範囲で考えて既約である。

(1) X^2+X+1
(2) X^2+3X+5
(3) $3X^3-X^2-1$
(4) X^3-X+1
(5) $4X^3-3X^2+2X-2$

(5.5) **命題 (アイゼンシュタインの既約判定法)** 整数係数の多項式 $f(X)=X^n+a_{n-1}X^{n-1}+\cdots a_1X+a_0$ が、ある素数 p に対して次の 2 条件を満たすとき、f は既約である。

(i) $a_0,a_1,\ldots,a_{n-1}$ は p の倍数。
(ii) a_0 は p^2 の倍数ではない。

Proof. (5.3) を用いずに係数の吟味だけで証明することもできるが、(5.3) を用いた証明を与える。

(i) と (ii) を満たすが、可約な多項式 f が存在したと仮定する。$f=gh$ ($\deg g=m$, $\deg h=n-m$, $1\le m<n$) とする。係数を p で法をとり $\overline{f}=\overline{g}\overline{h}$ と書くと、(i) より左辺は $\overline{f}=X^n$ であるが、これは X^mX^{n-m} としか分解しないから、$\overline{g}=X^m$, $\overline{h}=X^{n-m}$ である。すると g,h の定数項はともに p の倍数であるから、f の定数項は p^2 の倍数である。これは (ii) に反するから矛盾である。よって f は既約である。 □

(5.6) **例** 次の整数係数多項式は有理数係数の範囲で考えて既約である。

(1) x^2-2
(2) x^2-3x+3
(3) $x^3+6x^2-4x+18$
(4) x^3+3x^2+5x+5
(5) 素数 p に対して、$\Phi_p(x)=x^{p-1}+x^{p-2}+\cdots+x+1$ と定めると、既約多項式である。

§6 演習問題

(6.1) **問題** 次の問に答えよ。

(1) 33×44 を 7 で割った余りを求めよ。
(2) 33^{33} を 7 で割った余りを求めよ。

(6.2) **問題** n を非負整数とするとき次の問に答えよ。

(1) $2^{2n+3}-3^{2n+1}$ が 5 の倍数であることを証明せよ。
(2) $3^{3n}+5^{5n}+7^{7n}$ を 4 で割った余りが 3 であることを証明せよ。
(3) $3^{n+1}+5^{n+2}+8^{n+3}$ が 30 の倍数であることを証明せよ。

(6.3) **問題** ユークリッドの互除法を用いて、次の 2 数の最大公約数と最小公倍数を求めよ。
(1) $336,360$ (2) $448,588$

(6.4) **問題** 次の方程式を満たす、整数解 x,y を 1 組求めよ。

(1) $39x+28y=1$
(2) $28x-11y=1$
(3) $39x-11y=-3$

(6.5) **問題** 次の整数 n に対するオイラーの関数 $\phi(n)$ を求めよ。
(1) 11 (2) 21 (3) 512 (4) 840

(6.6) **問題** 101 が素数であることを用いて、99^{100} を 101 で割った余りを求めよ。

(6.7) **問題** 次の割り算の余りを求めよ。

(1) $30^{30}\div31$
(2) $18^{30}\div29$

(6.8) **問題** m, n を互いに素な正整数とする。

(1) 分数 m/n が有限小数になるための必要十分条件を書け。
(2) 分数 m/n が有限小数になるとき、小数第何位まであるかはどのようにすればわかるか。
(3) 有限小数になる分数 m/n であって、ちょうど小数第 4 位まである分数をひとつ言え。

(6.9) **問題** m, n を互いに素な正整数とする。

(1) 分数 m/n が循環小数になるための必要十分条件を書け。
(2) 純循環小数の定義を書け。
(3) 分数 m/n が純循環小数になるための必要十分条件を書け。
(4) 分数 m/n が循環小数になるとき、循環節の長さ e と、オイラーの関数 $\phi(n)$ の関係を言え。
(5) 5/21 の循環節の長さを求めよ。
(6) 10/21 の循環節の長さを求めよ。
(7) ローテーションして同じになる循環節は同じ種類であると言うことにする。21 を分母とする既約分数を循環小数で書いたとき、何種類の循環節が現れるか。

(6.10) **問題** 集合 R が環であるとは、演算が定まっていて、結合法則などを満たすことを言うのであった。環で定められていなくてはならないのは、どんな演算か。

(6.11) **問題** 次の集合は、環か否か。環でない場合は、どうして環ではないか答えよ。

(1) 正の整数全体
(2) 0 以上の整数全体
(3) 偶数全体
(4) 奇数全体
(5) 整数全体 $\mathbb{Z}$
(6) 有理数全体 $\mathbb{Q}$
(7) 実数全体 $\mathbb{R}$
(8) 複素数全体 $\mathbb{C}$
(9) 整数係数の多項式全体 $\mathbb{Z}[x]$
(10) 有理数係数の多項式全体 $\mathbb{Q}[x]$
(11) 実数係数の多項式全体 $\mathbb{R}[x]$
(12) 複素数係数の多項式全体 $\mathbb{C}[x]$

(6.12) **問題** 整数 m に対して、m を法とする剰余環 $\mathbb{Z}/(m)$ は、剰余類 $\overline{0}, \overline{1}, \ldots, \overline{m-1}$ からなる集合であった。剰余類 $\overline{k}$ も、集合として定めていたが、その定義を言え。

(6.13) **問題** 単元の定義を言え。また、次の環における単元をすべて書け
(a) $\mathbb{Z}$ (b) $\mathbb{Z}/(2)$ (c) $\mathbb{Z}/(3)$ (d) $\mathbb{Z}/(6)$ (e) $\mathbb{Z}[x]$ (f) $\mathbb{Q}$

(6.14) **問題** 零因子の定義を言え。また、次の環における零因子をすべて書け
(a) $\mathbb{Z}$ (b) $\mathbb{Z}/(2)$ (c) $\mathbb{Z}/(3)$ (d) $\mathbb{Z}/(6)$ (e) $\mathbb{Z}[x]$ (f) $\mathbb{Q}$

(6.15) **問題** 次の問に答えよ。

(1) 整域の定義を言え。
(2) 正整数 m に対して、剰余環 $\mathbb{Z}/(m)$ が整域であるための必要十分条件を言え。
(3) 次のうち整域をすべて言え。
(a) $\mathbb{Z}$ (b) $\mathbb{Z}/(2)$ (c) $\mathbb{Z}/(3)$ (d) $\mathbb{Z}/(6)$ (e) $\mathbb{Z}[x]$ (f) $\mathbb{Q}$

(6.16) **問題** 剰余環 $\mathbb{Z}/(11)$ において、$\overline{3}$ の逆元を求めよ。

(6.17)　**問題**　次の多項式は整数係数の範囲で既約か否か。また、有理数係数ではどうか。

(1) X^2+3X+1
(2) X^2+3X+3
(3) X^2+3X+9
(4) X^3+3X^2+6X+1
(5) X^3+3X^2-1
(6) X^4+3X^3+3

§7　問題の解答

(6.1) **の解答**　(1) $33\cdot 44\equiv 5\cdot 2\equiv 3 \pmod 7$. よって 3.
(2) $33^{33}\equiv 5^{33} \pmod 7$ である。5 のベキを小さい順に調べると、$5^6\equiv 1 \pmod 7$ がわかる。$33^{33}\equiv 5^{33}\equiv 5^{30+3}\equiv 5^3\equiv 125\equiv 6 \pmod 7$. よって 6.

(6.2) **の解答**　(1) mod5 で計算すると、$2^{2n+3}-32n+1=8\cdot 4^n-3\cdot 9^n\equiv 3\cdot 4^n-3\cdot 4^n\equiv 0 \pmod 5$ だから、5 の倍数である。
(2) $3^3\equiv 3 \pmod 4$, $5^5\equiv 1 \pmod 4$, $7^7\equiv 3 \pmod 4$ だから、mod4 で計算すると、$3^{3n}+5^{5n}+7^{7n}\equiv 3^n+1+3^n\equiv 2\cdot 3^n+1 \pmod 4$ である。n が偶数でも奇数でも $2\cdot 3^n\equiv 2 \pmod 4$ だから、$3^{3n}+5^{5n}+7^{7n}\equiv 2+1\equiv 3 \pmod 4$ となる。よって、$3^{3n}+5^{5n}+7^{7n}$ を 4 で割った余りは 3 である。
(3) $3^{n+1}+5^{n+2}+8^{n+3}$ が、2 の倍数、3 の倍数、5 の倍数であることを順に示せば、30 の倍数であることがいえる。まず、奇数 2 つと偶数の和だから 2 の倍数であることは明らかである。
次に mod 3 で計算すると、$3^{n+1}+5^{n+2}+8^{n+3}\equiv 2^{n+2}+2^{n+3}\equiv 2^n(4+8)\equiv 0 \pmod 3$ だから、3 の倍数である。
最後に mod 5 で計算すると、$3^{n+1}+5^{n+2}+8^{n+3}\equiv 3^{n+1}+3^{n+3}\equiv 3^n(3+27)\equiv 0 \pmod 5$ だから、5 の倍数である。以上より、証明された。

(6.3) **の解答**　(1)

$$360\div 336=1 \text{ あまり } 24,$$
$$336\div 24=14 \text{ あまり } 0.$$

だから最大公約数は 24. よって、最小公倍数は $360\times 336\div 24=5040$.
(2)

$$588\div 448=1 \text{ あまり } 140,$$
$$448\div 140=3 \text{ あまり } 28,$$
$$140\div 28=5 \text{ あまり } 0.$$

だから最大公約数は 28. よって、最小公倍数は $588\times 448\div 28=9408$.

(6.4) **の解答**　(1)

$$39\div 28=1 \text{ あまり } 11 \qquad \text{より } 11=39-28, \tag{a}$$
$$28\div 11=2 \text{ あまり } 6 \qquad \text{より } 6=28-11\cdot 2, \tag{b}$$
$$11\div 6=1 \text{ あまり } 5 \qquad \text{より } 5=11-6, \tag{c}$$
$$6\div 5=1 \text{ あまり } 1 \qquad \text{より } 1=6-5. \tag{d}$$

したがって、

$$\begin{aligned} 1 &\overset{\text{d}}{=} 6-5 \\ &\overset{\text{c}}{=} 6-(11-6)=6\cdot 2-11 \\ &\overset{\text{b}}{=} (28-11\cdot 2)\cdot 2-11=28\cdot 2-11\cdot 5 \\ &\overset{\text{a}}{=} 28\cdot 2-(39-28)\cdot 5=28\cdot 7-39\cdot 5. \end{aligned}$$

よって、$(x,y)=(-5,7)$.
(2)

$$28\div 11=2 \text{ あまり } 6 \qquad \text{より } 6=28-11\cdot 2, \tag{a}$$
$$11\div 6=1 \text{ あまり } 5 \qquad \text{より } 5=11-6, \tag{b}$$
$$6\div 5=1 \text{ あまり } 1 \qquad \text{より } 1=6-5. \tag{c}$$

したがって、

$$\begin{aligned} 1 &\overset{\text{c}}{=} 6-5 \\ &\overset{\text{b}}{=} 6-(11-6)=6\cdot 2-11 \\ &\overset{\text{a}}{=} (28-11\cdot 2)\cdot 2-11=28\cdot 2-11\cdot 5. \end{aligned}$$

よって、$(x,y)=(2,5)$.

(3)

$$\begin{aligned} 39\div 11=3 \text{ あまり } 6 \quad &\text{より } 6=39-11\cdot 3, \quad (a)\\ 11\div 6=1 \text{ あまり } 5 \quad &\text{より } 5=11-6, \quad (b)\\ 6\div 5=1 \text{ あまり } 1 \quad &\text{より } 1=6-5. \quad (c) \end{aligned}$$

したがって、

$$\begin{aligned} 1 &\overset{\text{c}}{=} 6-5 \\ &\overset{\text{b}}{=} 6-(11-6)=6\cdot 2-11 \\ &\overset{\text{a}}{=} (39-11\cdot 3)\cdot 2-11=39\cdot 2-11\cdot 7. \end{aligned}$$

よって、両辺 -3 倍すると、$(x,y)=(-6,-21)$ がわかる。

(6.5) の解答 (1) $\phi(11)=10$
(2) $\phi(21)=\phi(3)\phi(7)=2\cdot 6=12$
(3) $\phi(512)=\phi(2^9)=2^8(2-1)=256$
(4) $\phi(840)=\phi(8)\phi(3)\phi(5)\phi(7)=4\cdot 2\cdot 4\cdot 6=192$

(6.6) の解答 オイラーの定理より、$99^{100}=99^{\phi(101)}\equiv 1 \pmod{101}$.

(6.7) の解答 (1) オイラーの定理より、$30^{30}=30^{\phi(31)}\equiv 1 \pmod{31}$ だから、1.
(2) オイラーの定理より、$18^{28}=18^{\phi(29)}\equiv 1 \pmod{29}$ だから、$18^{30}\equiv 18^2\equiv 5 \pmod{29}$

(6.8) の解答 (1), (2) (2.11) (1) を見よ。(3) $1/80$ $(80=2^4\cdot 5)$

(6.9) の解答 (1) (2.4) (2) を見よ。(2) (2.10) を見よ。(3) (2.11) (2) を見よ。(4) (2.8) を見よ。(5) 6 (割り算すればわかる)。(6) 6 ((5) より自動的)。(7) $\phi(21)=12$ なので、$12\div 2=2$ 種類。

(6.10) の解答 和と積 (差も含めてもよいが、和と -1 との積があれば可能なので、含めなくてもよい)。

(6.11) の解答 (1) 環ではない (0 を含まない)。(2) 環ではない (差で閉じていない)。(3) 環ではない (1 を含まない)。(4) 環ではない (0 を含まない)。(5) から (12) はすべて環である。

(6.12) の解答 (1.12) を見よ。

(6.13) の解答 単元の定義は (4.3) を見よ。
(a) $1,-1$ (b) $\overline{1}$ (c) $\overline{1},\overline{2}$ (d) $\overline{1},\overline{5}$ (e) $1,-1$ (f) 0 以外すべて

(6.14) の解答 零因子の定義は (4.3) を見よ。
(a) 0 (b) $\overline{0}$ (c) $\overline{0}$ (d) $\overline{0},\overline{2},\overline{3},\overline{4}$ (e) 0 (f) 0

(6.15) の解答 (1) (4.3) を見よ。
(2) (4.7) と同じ条件 ($\mathbb{Z}/(m)$ が体であるのは、$\mathbb{Z}/(m)$ が整域であることと実は同値)。
(3) (a), (b), (c), (e), (f)

(6.16) の解答 $11x+3y=1$ の整数解を (互除法を用いるなどして) 求めると、$(x,y)=(2,-7)$ である。よって $11\cdot 2-3\cdot 7=1$ だが、これを mod11 すると、$3\cdot(-7)\equiv 1 \pmod{11}$ である。よって $\overline{3}$ の逆元は、$(\overline{3})^{-1}=\overline{-7}$ ($\overline{-7}$ を $\overline{4}$ に変形してもよい)。

(6.17) **の解答**　(5.2) により、整数係数の範囲での既約性と、有理数係数の範囲での既約性は同じであることに注意しておく。

　また、$\mathbb{Z}/(2)$ 係数の多項式として、X^2+X+1 や X^3+X^2+1 は既約である。なぜなら、可約ならば 1 次の因数があるはずだが、$X=\overline{0}$ を代入しても、$X=\overline{1}$ を代入しても 0 にならないから、X でも $X+\overline{1}$ でも割り切れないことがわかるからである。この事実は (5.3) を使うときに必要である。

　(1) から (6) まですべて既約である。(1) から (5) までは、(5.3) において $p=2$ とすればわかる。(2) と (6) は、(5.5) において $p=3$ とすればわかる。