佛教大学

代数学演習

まとめ

Notes by Kazuma MATSUDA

2019 年 7 月 23 日

1　数と演算　ー 加法と乗法 ー

1.1　自然数

公理 1.1 自然数の公理 (I)

任意の自然数 $a,\ b \in \mathbb{Z}$ が与えられたとき

$$a + b = c \tag{1.3a}$$
$$a \cdot b = d \tag{1.3b}$$

なる自然数 $c,\ d \in \mathbb{N}$ が一意に定まる.

公理 1.2 自然数の公理 (II)

任意の自然数 $a,\ b,\ c \in \mathbb{N}$ について

$$\text{交換則} : a + b = b + a\ , \qquad ab = ba \tag{1.8a}$$
$$\text{結合則} : (a + b) + c = a + (b + c)\ , \qquad (ab)c = a(bc) \tag{1.8b}$$
$$\text{分配則} : a(b + c) = ab + ac \tag{1.8c}$$

が成り立つ.

公理 1.3 自然数の公理 (III)

任意の自然数 $a \in \mathbb{N}$ について

$$a \cdot 1 = a$$

を満たす自然数 $1 \in \mathbb{N}$ が存在する.

定理 1.1 「1」の一意性

任意の $a \in \mathbb{N}$ について，$a \cdot 1 = a$ を満たす $1 \in \mathbb{N}$ は一意である．

定義 1.1 自然数の大小

任意の自然数 $a, b \in \mathbb{N}$ について $a < b$ となるとは $b = a + x$ なる自然数 $x \in \mathbb{N}$ が存在することである．

定理 1.2 自然数の大小関係

$a, b, c \in \mathbb{N}$ が $a < b$, $b < c$ を満たしているとする．このとき $a < c$ が成立する．

公理 1.4 自然数の公理 (IV)

任意の自然数 $a, b \in \mathbb{N}$ について $a < b$, $a = b$, $a > b$ のいずれかが成り立つ．

定理 1.3 等式の性質 (I)

$a, b, c \in \mathbb{N}$ について，次が成り立つ：

$$a = b \quad \Leftrightarrow \quad a + c = b + c \tag{1.9}$$

定理 1.4 等式の性質 (II)

$a, b, c \in \mathbb{N}$ について，次が成り立つ．

$$a = b \quad \Leftrightarrow \quad ac = bc \tag{1.10}$$

1.2 整数

1.2.1 自然数の引き算と 0

定義 1.2 自然数の減法

任意の自然数 $a, b \in \mathbb{N}$ について，引き算 $a - b$ の値は $a = x + b$ を満たす x の値である．即ち

$$a - b = x \quad \Leftrightarrow \quad a = x + b \tag{1.13}$$

公理 1.5 減法の入った結合則

$a, b, c \in \mathbb{N}$ について

$$a + (b - c) = (a + b) - c \tag{1.17}$$

が成り立つ．

公理 1.6 0 の公理

任意の自然数 $a \in \mathbb{N}$ について

$$a - a = 0 \tag{1.20a}$$
$$a + 0 = a \tag{1.20b}$$

を満たす 0 が存在する.

公理 1.7 引き算の入った分配則

$a, b, c \in \mathbb{N}$ について

$$a(b - c) = ab - ac \tag{1.23}$$

が成り立つ.

定理 1.5 0 の性質

$a \in \mathbb{N}$ について，次が成り立つ：

$$a \cdot 0 = 0 \tag{1.24}$$

定理 1.6 0 の一意性

任意の $a \in \mathbb{N} + \{0\}$ について，0 の公理 (公理 1.6) $a + 0 = a$ を満たす $0 \in \mathbb{N} + \{0\}$ は一意である.

1.2.2 負の数

公理 1.8 負の数

自然数 $a \in \mathbb{N}$ について，$a + x = 0$ を満たす x が存在し，それを $-a$ と書く.

定理 1.7 負の数の一意性

自然数 $a \in \mathbb{N}$ について，$a + x = 0$ を満たす x が一意に存在する.

命題 1.1 負の数の表記

$$(-1) \cdot a = -a \tag{1.30}$$

命題 1.2 減法の加法表記

$$a - b = a + (-b)$$

命題 1.3 $(-1)\cdot(-1) = 1$

$$(-1)\cdot(-1) = 1$$

1.3 環というのもの

公理 1.9 環の公理

二つの演算，加法「+」，減法「·」が定義された集合 R が環をなすとは，任意の元 $a,\ b,\ c \in R$ が次の公理を満たすときである．

$a + b \in R,\ a \cdot b \in R$ が一意に定まり，

・ 加法についての交換 : $a + b = b + a$ 則
・ 加法についての結合則 : $(a + b) + c = a + (b + c)$
・ 加法についての単位元 0_R の存在 : $a + 0_R = 0_R + a = a$
・ 加法について，任意の元 a についての逆元 a' の存在 : $a + a' = a' + a = 0_R$
・ 乗法についての結合則 : $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
・ 乗法についての単位元 1_R の存在 : $a \cdot 1_R = 1_R \cdot a = a$
・ 分配則 : $a \cdot (b + c) = a \cdot b + a \cdot c$ ，$(a + b) \cdot c = a \cdot c + b \cdot c$

また，特に

・ 乗法についての交換則 : $a \cdot b = b \cdot a$

が成り立つとき，環 R を可換環と呼び，そうでないときは非可換環と呼ぶ．

命題 1.4 零因子

$a,\ b \in \mathbb{Z}$ について，次が成り立つ：

$$ab = 0 \qquad \Rightarrow \qquad a = b \quad \text{または} \quad b = 0$$

上式が成り立つ環を整域と呼ぶ．

2　数と演算　— 除法 —

定義 2.1 割り算

任意の整数 $a \in \mathbb{Z}$ と，任意の自然数 $b \in \mathbb{N}$ について，割り算 $a \div b$ の値は $a = bx$ を満たす x の値である．即ち

$$a \div b = x \qquad \Leftrightarrow \qquad a = bx \tag{2.1}$$

公理 2.1 単位分数

自然数 $a \in \mathbb{N}$ について，$ax = 1$ を満たす数 x が存在し，それを $\dfrac{1}{a}$ と書く．

定理 2.1 逆元の一意性

自然数 $a \in \mathbb{N}$ について，$ax = 1$ を満たす x が一意に存在する．

定理 2.2 有理数表示

$$a \div b = x : \qquad a = bx \qquad \Leftrightarrow \qquad x = a \cdot \frac{1}{a} \tag{2.6}$$

2.2.1　有理数の算術

定理 2.3 約分

$$\frac{ac}{bc} = \frac{c}{b} \tag{2.8}$$

定理 2.4 通分

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \tag{2.9}$$

定理 2.5 有理数の掛け算

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} \tag{2.10}$$

定理 2.6 有理数割り算

$$\frac{\dfrac{a}{b}}{\dfrac{c}{d}} = \frac{ad}{bc} \tag{2.11}$$

2.2　有理数の少数表示

定義 2.2 有限小数

有理数 $\frac{n}{m}$ について，$\frac{n}{m} \times 10^k$ が整数となる自然数 $k \geq 1$ が存在するとき，$\frac{n}{m}$ を有限小数という．

命題 2.1 有限小数

$$\left(\text{有理数}\frac{n}{m}\text{が有限小数}\right) \quad \Leftrightarrow \quad \left(\text{有理数}\frac{n}{m}\text{の分母の素因数が 2, 5 のみ}\right)$$

命題 2.2 循環節の長さ

分母を p とする単位分数の循環節の長さは $p-1$ の約数となる．

2.2.1　有理数の連分数表示

命題 2.3 有理数

(有理数) ⇔ (連分数表示が有限で終わる)

2.3　無理数

2.3.1　無理数の連分数表示

2.3.2　代数的数と超越数

定理 2.7 2 次の代数的数

(2 次の代数的数) ⇔ (連分数表示に周期性がある)

定理 2.8 実数の表現形態としての連分数

任意の実数 a に対して，a に等しい値を持つ連分数が一意に存在する．また，この連分数は，a が有理数なら有限であり，無理数なら無限である．

2.4　体というもの

公理 2.2 体の公理

二つの演算「+」,「·」が定義された集合 K が体をなすとは K の任意の元 a, b, c が次の公理を満たすときである：

$a+b \in K$, $a \cdot b \in K$ が一意に定まり，

・ 加法についての交換則 : $a+b=b+a$
・ 加法についての結合則 : $(a+b)+c=a+(b+c)$
・ 加法についての単位元 0_K の存在 $a+0_K+0_K+a=a$
・ 加法について，任意の元 a についての逆元 a' の存在 : $a+a'=a'+a=0_K$
・ 乗法についての交換則 : $a \cdot b=b \cdot a$
・ 乗法についての結合則 : $(a \cdot b) \cdot c=a \cdot (b \cdot c)$
・ 乗法についての単位元 1_K の存在 $a \cdot 1_K=1_K \cdot a=a$
・ 乗法について，0_K を除く任意の元 a についての逆元 a'' の存在 : $a \cdot a''=a'' \cdot a=1_K$
・ 分配則 $a \cdot (b+c)=a \cdot b+a \cdot c$

公理 2.3 体の公理

環 R において，0_K 以外の元全てについて，乗法の下での逆元が存在するとき，R を体という．

2.4.1　いくつかの体

2.4.2　新しい体を作る

2.5　体と線型空間

公理 2.4 線型空間の公理

集合 V と体 K を考える．V が体 K 上の線型空間になるとは，V の任意の元 $\boldsymbol{v}$, $\boldsymbol{u}$, $\boldsymbol{w} \in V$ が次の小売を満たすことである：

・ 加法の演算が与えられる : $\boldsymbol{v}+\boldsymbol{u} \in V$
・ K の任意の元 k に対してスカラー倍が与えられる : $k\boldsymbol{v} \in V$
・ 加法についての交換則 : $\boldsymbol{v}+\boldsymbol{u}=\boldsymbol{u}+\boldsymbol{v}$
・ 加法についての結合則 : $(\boldsymbol{v}+\boldsymbol{u})+\boldsymbol{w}=\boldsymbol{v}+(\boldsymbol{u}+\boldsymbol{w})$
・ 加法についてゼロベクトル $\boldsymbol{0}$ の存在 : $\boldsymbol{v}+\boldsymbol{0}=\boldsymbol{0}+\boldsymbol{v}=\boldsymbol{v}$
・ 加法について，任意の元 $\boldsymbol{v}$ についての逆ベクトル $\boldsymbol{v}'$ の存在 $\boldsymbol{v}+\boldsymbol{v}'=\boldsymbol{v}'+\boldsymbol{v}=\boldsymbol{0}$
・ K の任意の元 k, l に関して次が成り立つ：
  ・ $k(l\boldsymbol{v})=(kl)\boldsymbol{v}$
  ・ $(k+l)\boldsymbol{v}=k\boldsymbol{v}+l\boldsymbol{v}$
  ・ $k(\boldsymbol{v}+\boldsymbol{u})=k\boldsymbol{v}+k\boldsymbol{u}$
  ・ $1_K\boldsymbol{v}=\boldsymbol{v}$

定義 2.3 体 $\mathbb{K}$ 上の線型空間 V の独立性

線型空間 V を考える．V のベクトル $\boldsymbol{v}_1, \boldsymbol{v}_2, \cdots, \boldsymbol{v}_m$ が体 K 上で線型独立とは，K の元 $k_1, k_2, \cdots, k_m$ を用いた関係式

$$k_1\boldsymbol{v}_1 + k_2\boldsymbol{v}_2 + \cdots + k_m\boldsymbol{v}_m = \boldsymbol{0}$$

が $k_1 = k_2 = \cdots = k_m = 0$ のときに限り満たされることである．

定義 2.4 体 $\mathbb{K}$ 上の線型空間 V の基底

線型空間 V を考える．また $\boldsymbol{v}_1, \boldsymbol{v}_2, \cdots, \boldsymbol{v}_m$ を V の線型独立なベクトルとする．このとき V の任意のベクトル $\boldsymbol{v}$ が K の元を展開係数とする $\boldsymbol{v}_1, \boldsymbol{v}_2, \cdots, \boldsymbol{v}_m$ の線型結合

$$\boldsymbol{v} = c_1\boldsymbol{v}_1 + c_2\boldsymbol{v}_2 + \cdots + c_m\boldsymbol{v}_m\,, \qquad c_1, c_2, \cdots, c_m \in K$$

で表されるとき，$\boldsymbol{v}_1, \boldsymbol{v}_2, \cdots, \boldsymbol{v}_m$ を線型空間の基底という．

3　整数についての基本的なこと

3.1　割り算とその余り

定理 3.1　整除の定理

任意の整数 $a,\ m\ \ (m \neq 0)$ について

$$a = mq + r\,, \qquad 0 \leq r < |m| \tag{3.4}$$

を満たす整数 (q, r) が一意に定まる．

3.2　約数

命題 3.1 整除関係

$a, b, c \in \mathbb{Z}$ とするとき，次が成り立つ：

$$a\big|b \quad \text{かつ} \quad b\big|a \qquad \Rightarrow \qquad |a| = |b| \tag{3.8}$$

$$a\big|b \quad \text{かつ} \quad b\big|c \qquad \Rightarrow \qquad a\big|c \tag{3.9}$$

$$c\big|a \quad \text{かつ} \quad c\big|b \qquad \Rightarrow \qquad c\big|(xa + yb) \qquad x,\ y \in \mathbb{Z} \tag{3.10}$$

3.3 n 進数展開

定理 3.2 基底 b (>1) による展開

$b>1$ を自然数とする．このとき，任意の自然数 n は

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b^1 + a_0 \tag{3.12}$$

と一意に表される．但し，a_i $(i = 0,\ 1,\ \cdots,\ k)$ は $0 \le a_i < b$ を満たす自然数であり，$a_k \neq 0$ である．

系 3.1 2 進数展開

全ての自然数は 2 の冪乗の和で表される．

3.4 最大公約数とユークリッドの互除法

3.4.1 ユークリッドの互除法

命題 3.2 最大公約数と行列表示

整数を成分とする 2×2 行列 $A = \begin{pmatrix} x & y \\ z & w \end{pmatrix}$ と整数 $a,\ b$ を用いて

$$\begin{pmatrix} a' \\ b' \end{pmatrix} = \begin{pmatrix} x & y \\ z & w \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}$$

によって整数 $a'b'$ を定める．このとき以下が成り立つ：

$$\cdot\ \gcd(a,b) \Big| \gcd(a',b') \tag{3.26}$$

$$\cdot\ |A| = \pm 1 \text{ ならば } \gcd(a,b) = \gcd(a',b') \tag{3.27}$$

3.5 1 次方程式の整数解

定理 3.3 1 次方程式の整数解

$$ax + by = k\ ,\ \ a,\ b,\ k \in \mathbb{Z}\ ,\ \ a \neq 0,\ b \neq 0,\ k \neq 0 \text{ が整数解 } (x,y) \text{ を持つ} \quad \Leftrightarrow \quad \gcd(a,b) \Big| k$$

4　素数

定義 4.1 素数

素数 p (>1) とは，1 と p 以外に正の約数を持たない整数のことである．

定義 4.2 合成数

素数でない正の整数で 1 を除いたものを合成数という．

補題 4.1 自然数は素数の積

$n \geq 2$ である任意の自然数は素数の積で表される．

補題 4.2 素数の性質

p を素数とし，a, b を整数とする．このとき $p|ab$ であれば $p|a$ または $p|b$ である．

補題 4.3　素数の性質

p を素数とし，a_1, a_2, $\cdots$, a_r を整数とする．このとき，$p|a_1a_2\cdots a_r$ であれば，p は因数 a_1, a_2, $\cdots$, a_r のうち少なくとも一つを割り切る．

定理 4.1 算術の基本定理

$n \geq 2$ である任意の自然数は素数 p_i を用いて $n = p_1p_2\cdots p_r$ と積の順番を除いて一意的に表される．

定理 4.2 素数

素数は無限個存在する．

定理 4.3 合成数

合成数 n を考える．このとき n は $\sqrt{n}$ を越えない素因数を持つ．

4.1　最大公約数と最小公倍数

5　整数の合同

5.1　合同式

定義 5.1 整数の合同

$a, b, m \in \mathbb{Z}$ に対して $a - b \in m\mathbb{Z}$ (即ち $m \mid (a-b)$) であるとき，

$$a \equiv b \mod m$$

と書き，a, b は m を法として合同であるという．そうでないときは $a \not\equiv b \mod m$ と書く．このような式を合同式という．

5.2　合同とは何か

5.3　合同式の性質

5.3.1　同値関係

定理 5.1 合同式の同値関係

1. 反射律 : $a \equiv a \mod m$
2. 対称律 : $a \equiv b \mod m \quad \Rightarrow \quad b \equiv a \mod m$
3. 推移律 : $a \equiv b \mod m$ かつ $b \equiv c \mod m \quad \Rightarrow \quad a \equiv c \mod m$

5.3.2　合同式の加減乗除

命題 5.1 合同式の性質

$a, b, c, d, m \in \mathbb{Z}$ が $a \equiv b,\ c \equiv d \mod m$ を満たすとき，次が成り立つ：

1. $a \pm c \equiv b \pm d \mod m$
2. $ac \equiv bd \mod m$

1. $a \equiv b \mod m \quad \Rightarrow \quad q \equiv b \mod m$
2. $k \neq 0$ のとき $a \equiv b \mod m \quad \Rightarrow \quad ka \equiv kb \mod m$
3. $k \neq 0$ のとき $a \equiv b \mod m \quad \Leftrightarrow \quad ka \equiv kb \mod mk$

命題 5.3　合同式の性質

$m \in \mathbb{N}, a, b, k \in \mathbb{Z}$ に対して，$\gcd(k, m) = 1$ のとき，次が成り立つ：

$$ka \equiv kb \mod m \qquad \Leftrightarrow a \equiv b \mod m$$

5.4 合同式を用いたいくつかの話題

5.5 何曜日？ ー 万年カレンダー

6 1 次合同方程式

定理 6.1 1 次合同方程式

$a \neq 0,\ b \neq 0 \in \mathbb{Z}$ とする合同方程式

$$ax \equiv b \mod m \tag{6.1}$$

は

1. $\gcd(a, m) = 1$ ならば，m を法として唯一つの解を持つ．
2. $\gcd(a, m) = d \neq 1$ で b が d で割りきれるならば，法 m として d 個の解を持つ．
3. $\gcd(a, m) = d \neq 1$ で b が d で割り切れないなたば，解は存在しない．

7 連立合同方程式

7.1 中国の剰余定理

定理 7.1 中国の剰余定理

連立合同式

$$\begin{cases} a_1 x \equiv b_1 \mod m_1 \\ a_2 x \equiv b_2 \mod m_2 \\ \quad \vdots \\ a_k x \equiv b_k \mod m_k \end{cases} \tag{7.2}$$

について，全ての i で $\gcd(a_i, m_i) = 1$ かつ全ての相異なる $i,\ j$ で $\gcd(m_i, m_j) = 1$ とするとき，(7.2) は法 $m_1 m_2 \cdots m_k$ の下で唯一の解を持つ．

命題 7.1 法の分割

$a,\ b$ を整数とする．互いに素な整数 m, n について次が成立する：

$$a \equiv b \mod mn \qquad \Leftrightarrow \qquad a \equiv b \mod m\ ,\ a \equiv b \mod n$$

定理 7.2 連立合同式

連立合同式について，次が成り立つ：

$$\begin{cases} x \equiv a \mod m \\ x \equiv b \mod n \end{cases} \text{が解を持つ} \quad \Leftrightarrow \quad a \equiv b \mod \gcd(m, n)$$

8　ウィルソンの定理

8.1　法 m の下での逆元

8.2　ウィルソンの定理

命題 8.1 有限体の逆元

p を素数とするとき

正の整数 a の法 p の下での逆元が a である　$\Leftrightarrow$　$a \equiv 1$ または $-1 \mod p$

定理 8.1 ウィルソンの定理

p を素数とすると，次が成り立つ：

$$(p-1)! \equiv -1 \mod p$$

9　フェルマーの小定理

定理 9.1 フェルマーの小定理

p を素数とし，a を p と互いに素な整数とするとき，次が成り立つ：

$$a^{p-1} \equiv 1 \mod p$$

10　オイラーの定理

定義 10.1 オイラー関数

自然数 $1, 2, \cdots, n$ の中にある n と互いに素な自然数の集合を考えたとき，その個数を $\varphi(n)$ と表す．この様に定まる自然数上の関数 φ をオイラー関数という．

定理 10.1 オイラーの定理

自然数 n と互いに素である自然数 a について，次が成り立つ：

$$a^{\varphi(n)} \equiv 1 \mod n \tag{10.7}$$

10.1 オイラー関数

命題 10.1 素数の冪乗

p^k と互いに素でない，それ以下の自然数は p^{k-1} 個ある．

定理 10.2 オイラー関数の公式

p を素数で，$k \geq 1$ とするとき，次が成り立つ：

$$\varphi(p^k) = p^k - p^{k-1} = p^k\left(1 - \frac{1}{p}\right) \tag{10.9}$$

定理 10.3 オイラー関数の公式

m, n を互いに素な自然数とするとき，次が成り立つ：

$$\varphi(mn) = \varphi(m)\varphi(n) \tag{10.10}$$

命題 10.2 オイラー関数の公式

自然数 n が ${p_1}^{a_1}{p_2}^{a_2}\cdots{p_k}^{a_k}$ で書けるとき，次が成り立つ：

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right)$$

11 RSA 暗号にむけて

11.1 法 m での逆元

命題 11.1 1 次合同方程式の解の構成

$$ax \equiv b \mod m\,, \qquad \gcd(a, m) = 1 \tag{11.3a}$$

の解は

$$x \equiv a^{\varphi(m)-1}b \mod m \tag{11.3b}$$

で与えられる．

11.2　法 m での k 乗根

$\gcd(b, m) = 1$ なる $b \in \mathbb{Z}$, $m \in \mathbb{N}$ を考える．$\bar{k}$ を法 $\varphi(m)$ の下での k の逆元

$$k\bar{k} \equiv 1 \mod \varphi(m) \tag{11.15a}$$

とすると

$$b^{k\bar{k}} \equiv b \mod m \tag{11.15b}$$

が成り立つ．

定理 11.1　法 m での k 乗根

$\gcd(b, m) = 1$ とする．このとき

$$x^k = b \mod m \tag{11.16a}$$

の解は一意に

$$x \equiv b^{\bar{k}} \mod m \tag{11.16b}$$

で与えられる．但し，$\bar{k}$ は法 $\varphi(m)$ の下での逆元，つまり $\gcd(k, \varphi(m)) = 1$ の下，$k\bar{k} \equiv 1 \mod \varphi(m)$ を満たす．

12　最後のメッセージ