代数入門演習　NO. 5　　2014. 10.21

5　素因数分解の一意性 (2), 素数, 合成数

5.1　一意的であるとは, 素因数分解の便利な記法

講義プリントの定理 4.3 で**初等整数論の基本定理**というものを教わったと思います. それは簡単にいうと次のものです.

定理 5.1 (初等整数論の基本定理)**.** 1 より大きい任意の自然数は素数の積に分解 (素因数分解) でき, さらにその分解の結果は順序を除いて一意的である.

分解できる, という意味はわかると思います. どんなに大きい数でも小さい素数から順に割っていけば, 最終的には素因数分解できそうですよね. **順序を除いて一意的である**というのは次のような意味です.

ある数を 2 つの全く別のやり方で素因数分解したとしても, その結果を並べ直すと必ず同じになる.

言い換えると, ある数を誰かが超斬新なやり方で素因数分解したとしても, その結果を並べ直すと, 小さい素数から割っていった素直な分解と同じになる, ということです. そんなの当たり前だと思うかもしれませんが, 当たり前だと堂々と言うためには証明もぜひ理解して下さい. (また, こういう分解の一意性が成り立たないような数の集合 (環) もあります. 詳しくは代数 I でやると思います.) この一意的である, という一見当たり前の性質はいろいろな命題の証明に使われます. 素因数分解の重宝な便利な記法を導入して実例を見てみましょう.

a を 0 でない任意の整数とする. $a \neq \pm 1$ ならば定理 5.1 により,

$$a = \pm \prod_{i=1}^{r} p_i^{e_i}$$

と一意的に分解できる. ここで, $p_1, \ldots, p_r$ はどの 2 つも相異なる素数, 指数 e_i は自然数. 一意性により指数 e_i は a の積の分解の中に素数 p_i (素因数) が何回現れるかという個数として確定する. そこで, 任意の素数 p に対して $v_p(a)$ を,

$$v_p(a) := \begin{cases} e_i, & (p = p_i\,(\exists i) \text{ のとき}), \\ 0, & (p \neq p_i\,(\forall i) \text{ のとき}) \end{cases}$$

により定義する. $v_p(a)$ を a の p **進付値 (p-adic valuation)** という. ($v_p(a)$ を $\mathrm{ord}_p(a)$ と書くこともある.) ここで $p \neq p_i\,(\forall i)$ のとき, p は a の素因数として現れないので, $v_p(a) = 0$ とおいている. $p^0 = 1$ だから,

$$a = \pm \prod_{p} p^{v_p(a)}$$

と書ける. ここで $\prod_p$ はすべての素数 p にわたる積である. この無限積は実際は有限積である. (素数は無限に多く存在すること思い出してほしい.) ± 1 は任意の素数 p で割り切れないから, $v_p(\pm 1) = 0$. したがって上の表示:

$$\pm 1 = \pm \prod_{p} p^{v_p(\pm 1)}$$

が成り立つ. 0 は素数 p により何回も割り切れるから ($0 = p^e \cdot 0$), 便宜上

$$v_p(0) := \infty$$

と定義する. このように各素数 p に対して写像

$$v_p\colon\ \mathbb{Z} \longrightarrow \mathbb{N}\cup\{0\}\cup\{\infty\},\quad a \longmapsto v_p(a)$$

が定義される. 例えば, $-360 = -2^3\cdot 3^2\cdot 5$ について,

$$v_2(-360) = 3,\quad v_3(-360) = 2,\quad v_5(-360) = 1.$$

p 進付値の性質を挙げる (**問題 5.1** も参照のこと). a, b を整数とする.

(I) 公式

$$v_p(ab) = v_p(a) + v_p(b) \tag{5.1}$$

が成り立つ.

証明. $a = 0$ または $b = 0$ のときは, 両辺は ∞ になるから (5.1) は成り立つ. ただし任意の整数 e に対して, $\infty + e = \infty$; さらに $\infty + \infty = \infty$ と規約する. そこで $a \neq 0$ かつ $b \neq 0$ と仮定する. a, b を素因数分解して,

$$a = \pm\prod_p p^{v_p(a)},\quad b = \pm\prod_p p^{v_p(b)}$$

と書く. このとき,

$$ab = \pm\prod_p p^{v_p(a)+v_p(b)}.$$

一方 $ab = \pm\prod_p p^{v_p(ab)}$ だから, **素因数分解の一意性**により $v_p(ab) = v_p(a) + v_p(b)$ となる. このように (5.1) が成り立つ. □

(II) **問題 4.4(1)** により,

$$a \mid b \iff \text{任意の素数 } p \text{ に対して } v_p(a) \leq v_p(b) \tag{5.2}$$

が成り立つ.

(III) p-進付値は $\mathbb{Z}$ から $\mathbb{Q}$ へ延長できる. x を 0 でない有理数として, $x = b/a$ $(a \in \mathbb{N}, b \in \mathbb{Z})$ と表わす [1]. そのとき,

$$v_p(x) := v_p(b) - v_p(a)$$

と定義する. この定義は a, b の取り方によらない (つまり, well-defined である). 実際, 別の分数表示 $x = b'/a'$ $(a' \in \mathbb{N}, b' \in \mathbb{Z})$ を取ると, $ab' = a'b$ であるから, (5.1) により

$$v_p(a) + v_p(b') = v_p(a') + v_p(b).$$

よって, $v_p(b') - v_p(a') = v_p(b) - v_p(a)$ となり表示の仕方によらないことがわかる. したがって各素数 p に対して写像

$$v_p\colon\ \mathbb{Q} \longrightarrow \mathbb{Z}\cup\{\infty\},\quad x \longmapsto v_p(x)$$

が定義される.

(IV) v_p を使うと $\mathbb{Q}$ の中で $\mathbb{Z}$ は次のように特徴付けられる: $x \in \mathbb{Q}$ について,

$$x \in \mathbb{Z} \iff \text{任意の素数 } p \text{ に対して } v_p(x) \geq 0 \tag{5.3}$$

が成り立つ. ただし任意の整数 e に対して, $\infty > e$ と規約する.

[1] x の分母・分子の共通因子を取り除くと, **問題 4.4(2)** により分母・分子を互いに素 $(\gcd(a,b) = 1)$ にできる. これを**既約分数**という.

証明. $x=0$ のときは上の規約から主張は成り立つ. それで $x\neq 0$ とし, $x=b/a$ $(a\in\mathbb{N}, b\in\mathbb{Z})$ と表わす. そのとき,

$$\begin{aligned} x\in\mathbb{Z} &\iff a\mid b \\ &\iff v_p(a)\leq v_p(b)\ (\forall p) \quad (\because (5.2)) \\ &\iff v_p(b)-v_p(a)\geq 0\ (\forall p) \\ &\iff v_p(x)\geq 0\ (\forall p). \end{aligned}$$

このように (5.3) を得る. □

定理 5.1 の応用例として, $\sqrt{5}$ が無理数であることの証明を復習する [2].

命題 5.2. $\sqrt{5}$ は無理数である.

証明. 背理法で示す. $\sqrt{5}$ が有理数であると仮定すると, ある自然数 a,b が存在して

$$\sqrt{5}=\frac{b}{a}$$

となる. 両辺に a をかけて 2 乗して $5a^2=b^2$ を得る. この両辺の 5-指数を見ると, 公式 (5.1) により,

$$1+2v_5(a)=v_5(5a^2)=v_5(b^2)=2v_5(b).$$

この左辺は奇数で, 右辺は偶数となり矛盾である [3]. よって $\sqrt{5}$ は有理数でない, つまり無理数である. □

この証明を使って次を 2 通りのやり方で示してみましょう. (細部は省略します.)

命題 5.3. $\dfrac{4-\sqrt{5}}{3}$ (>0) は無理数である.

[証明 1] (命題 5.2 の証明そのものをまねてみる.) $\dfrac{4-\sqrt{5}}{3}$ が有理数であると仮定すると, ある自然数 a,b が存在して

$$\frac{4-\sqrt{5}}{3}=\frac{b}{a}$$

となる. 変形すると,

$$5a^2=(3b-4a)^2$$

となる. この両辺の 5-指数を見ると, 公式 (5.1) により,

$$1+2v_5(a)=v_5(5a^2)=v_5((3b-4a)^2)=2v_5(3b-4a).$$

この左辺は奇数で, 右辺は偶数となり矛盾である. よって $\dfrac{4-\sqrt{5}}{3}$ は無理数である. □

[証明 2] (命題 5.2 を使う.) $x:=\dfrac{4-\sqrt{5}}{3}$ が有理数であると仮定する. 有理数は四則で閉じているので, $4-3x=\sqrt{5}$ も有理数となる. これは $\sqrt{5}$ が無理数であることに矛盾. よって $\dfrac{4-\sqrt{5}}{3}$ は無理数である. □

---

[2] 確認ですが, 無理数=「有理数でない実数」, $\sqrt{5}$ =「2 乗して 5 になる正の実数」です. そういう数が実数として存在することは微積 I でしつこくやったことですね.

[3] 整数 e を 2 で割ったとき, 余りが 0 ならば e を**偶数**, 余りが 1 ならば e を**奇数**という.

5.2 問題編

問題 5.1. p を素数とし, $a, b \in \mathbb{Z}$, $x, y \in \mathbb{Q}$ とする. 次を示せ.

(1) $v_p(a+b) \geq \min\{v_p(a), v_p(b)\}$. さらに $v_p(a) \neq v_p(b)$ のとき, 等号が成り立つことを示せ.

(2) $v_p(xy) = v_p(x) + v_p(y)$.

(3) $v_p(x+y) \geq \min\{v_p(x), v_p(y)\}$. さらに $v_p(x) \neq v_p(y)$ のとき, 等号が成り立つことを示せ.

(4) (**チャレンジ問題**) $x+y \in \mathbb{Z}$ かつ $xy \in \mathbb{Z}$ ならば $x, y \in \mathbb{Z}$.

問題 5.2. d を平方数でない自然数とすると, その平方根 $\sqrt{d}$ は無理数であることを示せ. ただし, **平方数とは整数の 2 乗として表される数のこと**である.

問題 5.3. 命題 5.2 の証明方法を使って, $\sqrt{3}+\sqrt{5}$ は無理数であることを示せ.

問題 5.4. $a, b \in \mathbb{N}$ とし, $\gcd(a,b) = 1$ を仮定する. 次を示せ.

(1) 積 ab が平方数ならば a と b は共に平方数である.

(2) $a \neq b$ とする. このとき,

$$\gcd(a+b, a-b) = \begin{cases} 2 & (a-b \text{ が偶数}), \\ 1 & (a-b \text{ が奇数}). \end{cases}$$

($a = b$ のときもこれは成り立つ. なぜか?)

問題 5.5. (**問題 2.3 の続き**) $a, b \in \mathbb{N}$ とする. 命題「$b^2 \mid a^2 \Longrightarrow b \mid a$」が正しければ証明を, 正しくなければ反例を与えよ.
(ヒント: p 進付値を使うと良い.)

問題 5.6. p を素数とする. $k = 1, 2, \cdots, p-1$ に対して $p \mid \binom{p}{k}$ を示せ. ただし,
$\binom{p}{k} := \dfrac{p!}{k!(p-k)!}$ は 2 項係数. また, p が合成数のときこれは成り立つか答えよ.
(ヒント: **講義プリントの命題 4.2** を使う.)

問題 5.7. 自然数 n に対して, n のすべての (正の) 約数の和を $S(n)$ と書く. 例えば, $S(6) = 1+2+3+6 = 12$ となる. 次の問いに答えよ.

(1) p が素数, $e \geq 0$ のとき, $S(p^e) = \dfrac{p^{e+1}-1}{p-1}$ となることを示せ.

(2) 自然数 m と n が互いに素, つまり $\gcd(m,n) = 1$ のとき, $S(mn) = S(m)S(n)$ が成り立つことを示せ.
(ヒント: **問題 4.4(2)** を使う.)

問題 5.8. 自然数 n に対して, n のすべての (正の) 約数の個数を $T(n)$ とする. 例えば, $T(6) = 4$ となる. $T(n)$ が奇数であるための n に関する必要十分条件を求めよ.

問題 5.9. (**チャレンジ問題**) 整数 p, $p+2$, $p+4$ が 3 つとも素数になるのは $p = 3$ の場合だけであることを示せ. また, p, $p+2$, $p+6$ が 3 つとも素数になるような p を 2 つ以上挙げよ.
(ヒント: p, $p+2$, $p+4$ を 3 で割ったときの余りに注意.)

問題 5.10. 自然数 n に対して, n 番目の素数を p_n と表す (つまり, $p_1 = 2$, $p_2 = 3$, $p_3 = 5, \cdots$). 次の問いに答えよ. [4]

(1) 自然数

$$11! + 2,\ 11! + 3,\ \cdots,\ 11! + 11$$

はすべて合成数であることを示せ.

(2) 不等式

$$p_{n+1} - p_n \geq 10$$

をみたす自然数 n が存在することを示せ.
(ヒント: $11! + 2 > p_n$ をみたす最大の番号 n を取れ.)

(3) 自然数 N が与えられたとき, この N に対して不等式

$$p_{n+1} - p_n \geq N$$

をみたす自然数 n が存在することを示せ.

問題 5.11. (**Fibonacci 数列**)　漸化式

$$f_0 = 0,\ f_1 = 1,\ f_n = f_{n-1} + f_{n-2}, \quad n \geq 2$$

により数列 $\{f_n\}_{n\geq 0}$ を定める. これは Fibonacci 数列と呼ばれている.

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	$\cdots$
f_n	0	1	1	2	3	5	8	13	21	34	55	89	144	233	377	$\cdots$

(1) 加法公式

$$f_{m+n} = f_{m+1}f_n + f_m f_{n-1}, \quad m \geq 0,\ n \geq 1$$

が成り立つことをを示せ.
(ヒント: $m \geq 0$ を固定して n に関する帰納法 (induction) を使う.)

(2) $m, n \geq 1$ のとき, $f_n \mid f_{mn}$ が成り立つことを示せ.
(ヒント: $n \geq 1$ を固定して, 小問 (1) を使って m に関する帰納法で示す.)

(3) $n \geq 1$, $n \neq 4$ とする. このとき, f_n が素数ならば n は素数である. 小問 (2) を使って証明せよ.
(ヒント: 対偶を示す.)

注意 5.1. Fibonacci 数列は多くの性質をもつことが知られている [5] . 例えば,

- $m \geq n \geq 3$ のとき, $f_n \mid f_m \Longrightarrow n \mid m$.　(**問題 5.11(2)** の逆.)
- $m, n \geq 1$ のとき, $\gcd(f_m, f_n) = f_d$. ここで $d := \gcd(m, n)$.　□

[4] 問題 5.10 から, 素数が「あまり密に (ミッチリ) 分布していない」ことがわかる. 一方で, 例えば素数の逆数和が発散することや, 素数定理が示すようにその分布は「それほど疎 (スカスカ) ではない」ことも知られている.

[5] 例えば次を参照せよ:
小林昭七,「なっとくする オイラーとフェルマー」, 第 2.2 節, 講談社, 2003.

発展問題

問題 5.12. 等式 $m^2 = 2^n + 1$ をみたす自然数 m, n をすべて求めよ.

問題 5.13. 次の問いに答えよ.

(1) n を自然数とし, $a_1, \ldots, a_n$ を整数とする. 方程式

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0$$

が有理数の解をもつならば, それは整数であることを示せ.

(2) 小問 (1) を使って, $\sqrt{2} + \sqrt{3}$ は無理数であることを示せ.

(3) 3 次方程式 $x^3 + 2x^2 + 10x - 5 = 0$ は有理数解をもたないことを示せ.

問題 5.14. a, b を自然数とする. $\gcd(a^2, b^2) = \gcd(a, b)^2$ は正しいか? 正しければ証明し, 正しくなければ反例を与えよ.

問題 5.15. n を自然数とする. 次の問いに答えよ.

(1) $\gcd(n-1, n^2+n+1)$ は 1 または 3 であることを示せ.

(2) $\gcd(2n, n+20)$ が取り得る値をすべて求めよ.

問題 5.16. 多項式 $f(T) = T$ に自然数を代入して行くと素数が無限個現れる. 多項式 $f(T) = 6(T-1) + 5 = 6T - 1$ に自然数を代入して行くと素数が無限個現れることを No.6 のプリントで見る予定である. 合成数に対してもこの類似が成り立つことを見よう.

次数 n が 1 次以上の整数係数多項式

$$f(T) = a_n T^n + a_{n-1} T^{n-1} + \cdots + a_1 T + a_0, \quad a_n > 0$$

を考える. ここで最高次の係数 a_n は正と仮定する.

(1) ある実数 $x_1 > 0$ が存在して, 関数 $f(x)$ は区間 $[x_1, \infty)$ で $f(x) > 0$ となることを示せ.

(2) ある実数 $x_2 > x_1$ が存在して, 関数 $f(x)$ は区間 $[x_2, \infty)$ で狭義単調増加, かつ $f(x) > 1$ となることを示せ. (ヒント: $f'(x) > 0$ となればよい.)

(3) 整数係数多項式 $F(T)$ が存在して, すべての自然数 m に対して

$$f(m + f(m)) = f(m) + f(m)F(m) = f(m)(1 + F(m))$$

をみたすことを示せ. (ヒント: 二項定理を使って $f(m + f(m))$ を計算せよ.)

(4) 小問 (2), (3) を使って, 多項式 $f(T)$ に自然数 m を代入して行くと合成数が無限個現れることを示せ. (ヒント: $x_2 > 0$ を小問 (2) の実数とし, $m > x_2$ をみたす自然数 m を取ってみよ. 関数 $f(x)$ の区間 $[x_2, \infty)$ 上の狭義単調増加性を使う.)