高等学校数学での整数の性質についての注意 2

–素元と既約元およびユークリッド整域–

*田　谷　久　雄

On new curriculum “property of the integers” of high school mathematics 2
– prime elements, irreducible elements and Euclidean domain –

TAYA Hisao

概　要

本稿では，高校数学の新課程で新しく登場した「整数の性質」に関連した話題として，素数の定義と性質に起因とする既約元と素元について述べると共に，整数の割り算原理（除法定理）から素因数分解とその一意性までの流れの出発点であるユークリッド整域について簡単な注意を与える．

In this paper, we will mention irreducible elements and prime elements which come from the definition of and a property of prime numbers, respectively. Also, we will make a simple remark about the definition of Euclidean domain, which is the starting point from Euclidean division to Unique Factorization Theorem.

Key words：high school mathematics (高等学校数学)
property of the integers (整数の性質)
prime numbers (素数)
prime decomposition (素因数分解)
Euclidean division (割り算原理)

1　序

本稿は [Tay15] の続編であり，平成 21 年 3 月の高等学校学習指導要領の改訂により平成 24 年度から年次進行で実施された新高等学校学習指導要領等 ([Mb09] 参照) で新たに設けられた「数学 A」の「整数の性質」に関して，数学的な側面からその取り扱いにおける注意点を述べるものであり，今回はさらに素元と既約元について理解を深めると共に，ユークリッド整域についても述べてみたい．ここで述べることは，専門書ではあまり触れられていないことである．

*宮城教育大学数学教育講座

2　素元と既約元

前稿では，素数の定義と素因数分解の一意性について注意すべき点を述べた．そのポイントは，素数の定義は既約元性と呼ばれる性質によって定義されているのに対し，素因数分解の一意性は素数の素元性と呼ばれる性質を利用して証明されるということであり，この 2 つの性質が直接結びつくことは自明なことでなく，証明が必要であるということであった．しかし，教科書ではその部分の記述が曖昧であるため，正しい理解がないと誤解を生じる危険性があり，同時に教えるにあたってもこの点は注意が必要になるということで

ある．

ここでもう一度この既約元性と素元性を振り返ってみる．素数の定義は教科書でも述べられているように「2 以上の自然数で，1 とそれ自身以外に正の約数をもたない数」を素数という．整数 a と b について a が b の倍数であるとき，つまり，$a = bc$ となる整数 c が存在するとき，$b \mid a$ と書くことにすれば，素数の定義は以下の通りである．

定義 2.1 自然数 p が素数であるとは，p は 2 以上であり，かつ，a を自然数とするとき，

$$a \mid p \text{ ならば } a = 1 \text{ または } a = p$$

を満たすことである．

この性質は，次の既約元の定義のもとになるものであり，これをここでは既約元性と呼ぶ．

定義 2.2 (既約元 (その 1)) R を整域とする（整域の定義については次節で確認する）．R の零元でも単元でもない元 π が既約元であるとは，

$$\alpha \mid \pi \text{ ならば } \alpha = \text{単元または} \alpha = \pi \times \text{単元}$$

を満たすこととする．ただし $\alpha \in R$ である．

ここで，零元とは加法に関する単位元 0，つまり，任意の $a \in R$ について，

$$a + 0 = 0 + a = a$$

をみたす $0 \in R$ のことである．なお，乗法に関する単位元，つまり，任意の $a \in R$ について，

$$a \cdot 1 = 1 \cdot a = a$$

をみたす $1 \in R$ のことを単に R の単位元という．また，単元とは R において乗法に関する逆元をもつ元のこと，つまり，$a \in R$ が単元であるとは，

$$a \cdot b = b \cdot a = 1$$

となる $b \in R$ が存在することである．このような元 b は存在すれば唯一つであり，a の逆元と呼ばれ，a^{-1} で表す．ここで述べた零元，単位元，単元という用語の定義は R を整域より広い範疇の可換環としたときにも全く同様である（可換環の定義については次節で確認する）．

たとえば，整数全体の集合 $\mathbb{Z}$ において，零元は通常の 0，単位元は通常の 1，単元は ± 1 となる．また，単元 ± 1 の逆元は $1^{-1} = 1$，$(-1)^{-1} = -1$ である，なお，既約元の定義をそのまま当てはめれば，-2 や -3 も素数と呼んでよいことになるが，符号の違いは素因数分解において $+$ を付けるか $-$ を付けるかだけの違いであるので，正の整数だけを考えて素数の定義としている（負の数を知らない段階で素数は登場することも起因する）．

一方，素因数分解の一意性を示すときにどのような素数の性質が必要であるかは教科書では触れられていないが，次の性質を利用することになる．

命題 2.3 p を素数とするとき，整数 a, b に対して

$$p \mid ab \text{ ならば } p \mid a \text{ または } p \mid b$$

が成り立つ．

この性質は，整数を積に細分化し続けたとき最後に残るものが素数であるという素因数分解における素数のイメージとマッチしているため，何の証明もなしに利用できる性質として高校までの数学では取り扱われている感がある．しかし，これは素数の定義ではないので，明らかに証明が必要な素数の性質である．この性質は，次の素元の定義のもとになっているものであり，これをここでは素元性と呼ぶ．

定義 2.4 (素元) R を可換環とする．R の零元でも単元でもない元 π が素元であるとは，

$$\pi \mid \alpha\beta \text{ ならば } \pi \mid \alpha \text{または} \pi \mid \beta$$

を満たすこととする．ただし $\alpha, \beta \in R$ である．

素数がこの素元性の性質をもつことは前編で示しているが，難しいことではないので，ここでもその証明の一例を振り返っておこう．

(命題 2.3 の証明) 整数 a, b について $p \mid ab$ であるとする．このとき，$p \mid a$ であれば主張は自明である．そこで，$p \nmid a$ であるとする．p が素数であるので，このことは a と p は互いに素であることを意味する．したがって，2 元 1 次不定方程式の性質によれば，

$$ka + lp = 1$$

となる整数 k, l が存在する．この両辺に b を掛ければ，

$$p \mid kab + lpb = b$$

が従うので，$p \mid b$ となる．つまり，$p \nmid a$ のときには常に $p \mid b$ が成り立つ．以上より，素数 p は $p \mid ab$ ならば $p \mid a$ または $p \mid b$ を満たすことがわかる． □

なお，ここで利用した 2 元 1 次不定方程式の性質は，高等学校「数学 A」の「整数の性質」でも扱っている内容で，ユークリッドの互除法，より原点に返れば，整数の割り算原理を利用すれば示せる性質で，もちろん素因数分解とその一意性などは利用せずに証明できる．したがって，高校生でも理解できる範囲の内容であり，そうでなくとも教師にとっては理論的な流れの一つとして確認しておくと役立つであろう．

素元と既約元，および，既約元による既約元分解とその一意性（素因数分解とその一意性の一般化）については，次の定理が成り立つ（代数学の本，たとえば，[Kid07] 参照）．

命題 2.5 R を既約元分解（素因数分解の一般化）が可能な整域とする．このとき次は同値である．

(1) 素元と既約元は一致する．
(2) 既約元分解は一意的である．

この命題から，既約元が素元の性質を持たなければ，既約元分解の一意性は成り立たないことがわかる．したがって，素因数分解の一意性においても素数が素元の性質をもつことが本質的なのである．前編 [Tay15] で紹介したが，整域では既約元と素元の概念は必ずしも一致しない．このことは，整域において既約元による既約元分解の一意性が成り立つとは限らないことに繋がる．したがって，整数の性質に関する命題がどのような事柄に起因したものかを知ることは大切なことである．

3 既約元の定義

この節では既約元の定義について注意を述べる．その前に可換環と整域の定義を確認しておこう．

定義 3.1 (可換環) 集合 R に加法 $+$ と乗法 $\cdot$ が定義されていて，次の条件 (1) から (8) を満たすとき，R を可換環という．

(1) (加法の結合律) 任意の $a, b, c \in R$ に対して $(a+b)+c = a+(b+c)$ が成り立つ．
(2) (零元の存在) 任意の $a \in R$ に対して $a+0 = 0+a = a$ となる零元と呼ばれる元 $0 \in R$ が存在する．
(3) (加法の逆元の存在) 任意の $a \in R$ に対して $a+b = b+a = 0$ となる a の逆元と呼ばれる元 $b \in R$ が存在する．
(4) (加法の交換律) 任意の $a, b \in R$ に対して $a+b = b+a$ が成り立つ．
(5) (乗法の結合律) 任意の $a, b, c \in R$ に対して $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ が成り立つ．
(6) (単位元の存在) 任意の $a \in R$ に対して $a \cdot 1 = 1 \cdot a = a$ となる単位元と呼ばれる元 $1 \in R$ が存在する．
(7) (乗法の交換律) 任意の $a, b \in R$ に対して $a \cdot b = b \cdot a$ が成り立つ．
(8) (分配律) 任意の $a, b, c \in R$ に対して $a \cdot (b+c) = a \cdot b + a \cdot c$ および $(a+b) \cdot c = a \cdot c + b \cdot c$ が成り立つ．

なお，(7) の乗法の交換律を除く，(1)〜(6) と (8) を満たすとき，R を非可換環という．

可換環の代表的な例は，整数全体の集合 $\mathbb{Z}$ や実数係数の多項式全体の集合 $\mathbb{R}[x]$ である．次に定義 2.2 で登場した整域について確認しておこう．

定義 3.2 (整域) 可換環 R が 0 以外の零因子をもたない，つまり，$a, b \in R$ に対して

$$ab = 0 \text{ ならば } a = 0 \text{ または } b = 0$$

が成り立つとき，R を整域という．

可換環の代表例である $\mathbb{Z}$ や $\mathbb{R}[x]$ は整域である．一方，「整数の性質」が新しく導入されたことによって高等学校数学から姿を消した 2 次の正方行列全体の集合は，非可換環であり（$AB \neq BA$ となる 2 次の正方行列 A, B が存在する），さらに零因子をもつので（A も B も零行列ではないが AB が零行列となる 2 次の正方行列 A, B が存在する），整域ではない非可換環の代表例である．

可換環と整域の定義を確認したところで，既約元の定義について述べていく．

先の節で素数の定義に起因する概念として既約元の定義を述べた．しかし，この定義は代数学のテキストで学んだ既約元の定義と違うのではないかと思った方もいるのではないだろうか．それはおそらく次のような定義がテキストに書かれていたためであろう．

定義 3.3 (既約元 (その 2)) R を可換環とする．R の零元でも単元でもない元 π が既約元であるとは，$\alpha, \beta \in R$ について，

$$\pi = \alpha\beta \text{ ならば } \alpha = \text{単元または} \beta = \text{単元}$$

を満たすこととする．

定義 2.2 と 3.3 とを比べると，表現は微妙に違う．これらの関係はどのようになっているのであろうか．実は，整域においては両者の定義は一致する．しかし，可換環においては若干注意が必要である．このことを説明していく．

まず，次のことは簡単にわかる．

命題 3.4 可換環 R において，既約元 (その 2) の定義を満たす元は（R を可換環としても）既約元 (その 1) の定義を満たす．

(証明) $\pi \in R$ を既約元 (その 2) の定義を満たす既約元とし，$\alpha \in R$ について $\alpha \mid \pi$ とする．このとき，α が単元ならば既約元 (その 1) の定義を満たす．そこで，α は単元でないとする．最初の仮定より $\pi = \alpha\beta$ となる $\beta \in R$ が存在する．既約元 (その 2) の定義より必然的に β は単元でなければならない．よって，$\pi = \alpha \times$ 単元 とかける．ここで，単元には逆元が存在し，その逆元も単元であるので，$\alpha = \pi \times$ 単元 が得られる．したがって，π は既約元 (その 1) の定義を満たすことがわかる． □

しかしながら，次の例からわかるように，R を可換環と仮定した命題 3.4 の逆は成り立たない．

例 3.5 整数を 6 で割ったときに余りとして現れる整数全体の集合を $R = \{0, 1, 2, 3, 4, 5\}$ とする．このとき，通常の整数としての和を 6 で割ったときの余りの値を R での和と定め，通常の整数としての積を 6 で割ったときの余りの値を R での積と定めると，R は可換環になる．R は整数 $\mathbb{Z}$ の法 6 による剰余環と呼ばれ，記号で $\mathbb{Z}/6\mathbb{Z}$ と表される．たとえば，$1+3=4, 3+5=2, 5+0=5$ であり，$1\cdot 5=5, 2\cdot 5=4, 5\cdot 5=1$ となる．さらに，$3 \neq 0$ と $4 \neq 0$ の積は $3\cdot 4 = 0$ であるので，$R = \mathbb{Z}/6\mathbb{Z}$ は整域ではない可換環であることに注意する．すぐにわかるように，$R = \mathbb{Z}/6\mathbb{Z}$ において，0 が零元，1 が単位元，1 と 5 が単元である．$R = \mathbb{Z}/6\mathbb{Z}$ において，結果が 3 となる 2 つの元の積を調べれば，$3 = 1\cdot 3 = 3\cdot 1 = 3\cdot 3 = 3\cdot 5 = 5\cdot 3$ ですべてである．よって，3 は既約元 (その 1) の定義を満たすが，3 は $R = \mathbb{Z}/6\mathbb{Z}$ の単元ではないので既約元 (その 2) の定義は満たさない．したがって，可換環では命題 3.4 の逆は一般には成り立たない．

例 3.5 では整域でない可換環を例としてあげた．整域でない可換環と整域との違いは，零因子と呼ばれる元，つまり，a も b も 0 ではないがその積 ab が 0 となる元が存在するかしないかである（定義 3.2 参照）．そこで，既約元の定義において，π は零因子でも単元でもない元としてみよう．すると，実は両者の定義は一致する．

命題 3.6 可換環 R において，R の零因子でも単元でもない元 π について，次の 2 条件は同値である．

(1) (既約元 (その 1)) $\alpha \in R$ について，$\alpha \mid \pi$ ならば $\alpha =$ 単元 または $\alpha = \pi \times$ 単元 である．
(2) (既約元 (その 2)) $\alpha, \beta \in R$ について，$\pi = \alpha\beta$ ならば $\alpha =$ 単元 または $\beta =$ 単元 である．

(証明) (2) $\Rightarrow$ (1) が成り立つことは命題 3.4 で示した．よって，この逆を示す．

π は (1) を満たす元とし，$\alpha, \beta \in R$ について $\pi = \alpha\beta$ とする．仮に (2) は満たさない，つまり，α も β も単元でないとして矛盾を導く．まず $\alpha \mid \pi$ かつ $\beta \mid \pi$ より，(1) を満たすことから $\alpha = \pi \times$単元 かつ $\beta = \pi \times$単元 でなければならない．つまり，ある単元 $\delta, \varepsilon \in R$ があって $\alpha = \pi\delta$, $\beta = \pi\varepsilon$ と書ける．よって，$\pi = \pi^2\delta\varepsilon$ となる．このとき，$\pi(1 - \pi\delta\varepsilon) = 0$ となるが，仮定より π は単元ではないので $1 \neq \pi\delta\varepsilon$ より，π は零因子となる．しかし，これは π の仮定に矛盾する．よって，π は (2) を満たし，(1) $\Rightarrow$ (2) が示せた． □

とくに，R が整域であれば，零因子は零元だけであるので，次が成り立つ．

命題 3.7 R を整域とし，π を零元でも単元でもない R の元とするとき，π が既約元 (その 1) の定義により既約元となることと既約元 (その 2) の定義により既約元となることは同値である．

以上より，既約元 (その 1) の定義と既約元 (その 2) の定義はそのままでは本質的に微妙な差はあるが，R を整域と仮定するか，または，既約元の対象となる元を零因子でも単元でもない元とすれば，全く同値なものとなる．

4　ユークリッド整域

第 2 章で素数の既約元性（定義）から素元性（命題 2.3）が従うことを 2 元 1 次不定方程式の性質を利用して証明した．この性質はユークリッドの互除法から従うものであるが，ユークリッドの互除法は次の割り算原理と最大公約数の定義から得られる．

定理 4.1 (割り算原理（除法定理）) a と b を整数とし，$b \neq 0$ とする．このとき，

$$a = bq + r, \quad 0 \leq r < |b|$$

を満たす整数 q, r がただ一組存在する．

この節では，割り算原理が成り立つ整域であるユークリッド整域について簡単な注意を述べる．

ユークリッド整域の定義をいくつかのテキストで調べると，微妙に違っていることがある．代表的なものを以下にあげてみる．

定義 4.2 (ユークリッド整域の定義 1) R を整域とし，R から R の零元を除いた集合を R_0 とする．つまり，$R_0 = R - \{0\}$ とする．このとき，R_0 から自然数全体の集合 $\mathbb{N}$ への写像 φ で次の条件を満たすものが存在するとき，R をユークリッド整域という．

(1) R の元 a と元 $b \neq 0$ に対して，

$$a = bq + r,\ r = 0 \text{ または } \varphi(r) < \varphi(b)$$

となる R の元 q, r が存在する．

定義 4.3 (ユークリッド整域の定義 2) R を整域とする．R から 0 以上の整数全体の集合 $\mathbb{Z}_{\geq 0}$ への写像 φ で次の条件を満たすものが存在するとき，R をユークリッド整域という．

(1) R の元 a について，$\varphi(a) = 0$ と $a = 0$ は同値である．
(2) R の元 a と元 $b \neq 0$ に対して，

$$a = bq + r, \quad \varphi(r) < \varphi(b)$$

となる R の元 q, r が存在する．

定義 4.4 (ユークリッド整域の定義 3) R を整域とし，R から R の零元を除いた集合を R_0 とする．つまり，$R_0 = R - \{0\}$ とする．このとき，R_0 から 0 以上の整数全体の集合 $\mathbb{Z}_{\geq 0}$ への写像 φ で次の条件を満たすものが存在するとき，R をユークリッド整域という．

(1) R の零でない元 a と b について，$\varphi(a) \leq \varphi(ab)$ となる．
(2) R の元 a と $b \neq 0$ に対して，

$$a = bq + r,\ r = 0 \text{ または } \varphi(r) < \varphi(b)$$

となる R の元 q, r が存在する．

なお，ユークリッド整域の定義では，割り算原理に相当する条件において q と r はただ一組であることを要求していない．一意的でなくとも存在しさえすればよいのである．

さて，これらの定義を比べると，φ の定義域と値域は多少違うが，これは簡単に調整できる差であり，ここで取り上げたいことは，定義 4.3 と 4.4 では 2 つの条件が課されているという点である．そして，実は，これら 2 つの条件のうち，定義 4.3 と 4.4 における条件 (1) は不要であるということを述べる．

そのために，定義 4.2 を標準の定義とし，定義 4.2 を満たせば，定義 4.3 も 4.4 も満たすことを確認する．

まず，定義 4.3 の条件 (1) についてであるが，定義 4.2 を満たす φ が存在すれば，R の元 $a \neq 0$ に対して $\varphi(a) > 0$ であるので，φ の定義域と値域を広げて，R から 0 以上の整数全体の集合 $\mathbb{Z}_{\geq 0}$ への写像 φ として $\varphi(0) = 0$ と定めれば，これで定義 4.3 の条件 (1) を φ が満たす．このと

き，同時に定義 4.3 の条件 (2) も満しているので，定義 4.2 の φ が存在すれば定義 4.3 の φ も存在する．

注意 4.5 定義 4.3 のように，φ を R から 0 以上の整数全体の集合 $\mathbb{Z}_{\geq 0}$ への写像として，さらに，条件 (2) の余りの条件を $\varphi(r) < \varphi(b)$ としていれば，そもそも条件 (1) は不要である．なぜならば，ρ を R から $\mathbb{Z}_{\geq 0}$ への写像で定義 4.3 の条件 (2) を満たすものとする．このとき，R の元 $b \neq 0$ について，$a \in R$ を補助的にとれば，条件 (2) より $\rho(r) < \rho(b)$ となる R の元 r が存在する．よって，必然的に ρ は 0 のとき最小値をとり，かつ，最小値をとる R の元は 0 だけとなる．そこで，R の元 a に対して写像 φ を $\varphi(a) = \rho(a) - \rho(0)$ により定めれば，φ は R から $\mathbb{Z}_{\geq 0}$ への写像であり，条件 (1) を満たすと共に，条件 (2) の余りの不等式も満足することがわかる．つまり，定義 4.3 の 2 条件を満たす．したがって，条件 (1) は必要ないということになる．

次に，定義 4.4 の条件 (1) についてみてみる．まず，定義 4.2 を満たす φ が存在したとする（このことは，定義 4.4 の条件 (2) を満たす φ が存在するとしても同じである）．このとき，R の零でない元 a に対して，

$$\rho(a) = \min_{b \in R, ab \neq 0} \varphi(ab)$$

によって写像 ρ を定める．ここで，min は $ab \neq 0$ となる R の元 b をすべて動かしたときの $\varphi(ab)$ のとる値の最小値を表す．これは R_0 から $\mathbb{N}$ への写像であり，よって，とくに R_0 から $\mathbb{Z}_{\geq 0}$ への写像でもある．

さて，R の元 a と元 $b \neq 0$ に対して，ρ の定義より，$bc \neq 0$ で $\rho(b) = \varphi(bc)$ となる $c \in R$ が存在する．このとき，φ の定義より，$a = (bc)q + r$ をみたし, かつ，$r = 0$ または $\varphi(r) < \varphi(bc)$ となる R の元 q, r が存在する．これを $a = b(cq) + r$ とみれば，$\rho(r) \leq \varphi(r) < \varphi(bc) = \rho(b)$ より，ρ は定義 4.4 の条件 (2) を満たす．さらに，任意の $a, b \in R$ について，$ab \neq 0$ ならば，ab は a の倍元となることと ρ の作り方より $\rho(a) \leq \rho(ab)$ が成り立つ．したがって，とくに R が整域であれば，ρ は定義 4.4 の条件 (1) を満たす．以上より，定義 4.2 を満たす φ が存在すれば，定義 4.4 を満たす φ も存在することがわかる（論文 [Sam71] 参照）．

以上のことは，高校数学という立場で眺めると少々難しいことに思えるかもしれないが，ユークリッド整域は単項イデアル整域であり，単項イデアル整域は一意分解整域（既約元による既約元分解とその一意性が成り立つ整域）となり，この流れによって整数の割り算原理から素因数分解とその一意性が成り立つことが一般的に理解できるので，その出発点としてのユークリッド整域の定義についてここで取り上げた.「整数の性質」のバックグラウンドを学ぶことは教科書の内容を理解する上で大切である．本稿前半の内容と合わせて参考となれば幸いである．

前編の訂正　前編 [Tay15] の訂正を与える．

1. p.101 の定義 2.2 において,「R を可換環とする」を「R を整域とする」に訂正．これは今回の第 3 章の内容とも関係する．
2. p.107 で登場するイデアル「(20)」を「$(20)\mathfrak{p}_\infty$」に訂正（4 箇所）．ここで，$\mathfrak{p}_\infty$ は $\mathbb{Q}$ に存在する唯一つの無限素点（その実体は共役写像）であり，p.107 の同型は

$$C_{\mathbb{Q}}((20)\mathfrak{p}_\infty)/H_{\mathbb{Q}}((20)\mathfrak{p}_\infty) \simeq \mathrm{Gal}(\mathbb{Q}(\sqrt{-5})/\mathbb{Q})$$

となる（無限素点も分岐する）．

参考文献

[Kid07] 木田雅成, 数理 · 情報系のための整数論講義, SGC ライブラリー 58，サイエンス社, 2007 年 9 月.

[Tay15] 田谷久雄, 高等学校数学での整数の性質についての注意 –素数の定義と素因数分解およびその拡がり–，宮城教育大学紀要, 第 **50** 号, 2015, pp. 99-107.

[Mb09] 文部科学省, 高等学校学習指導要領解説, 平成 21 年 12 月.

[Sam71] Samuel, Pierre. *About Euclidian Rings*, Journal of Algebra **19** (1971), pp.282-301.

田谷 久雄 (TAYA Hisao)
宮城教育大学 数学教育講座
980-0845 仙台市青葉区荒巻字青葉 149
E-mail : taya@staff.miyakyo-u.ac.jp

（平成29年 9 月29日受理）