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－

*田　谷　久　雄

On new curriculum "property of the integers" of high school mathematics
－the definition of prime numbers, prime decomposition and its development－

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」について，素数の既約元性と素元性という2つの性質に焦点を当て，純粋数学的な観点から注意すべき事柄を述べる．また，これらの素数の性質の一つの発展した題材として，素イデアルによる分解とその一意性の出現，および，代数的整数論における類体論の一つの見方を概説する．

In this paper, we will mention a remarkable thing about the new curriculum "property of the integers" of high school mathematics, focusing on two properties of prime numbers, i.e., the properties as "irreducible elements" and as "prime elements", from a purely mathematical point of view. In addition, we will explain unique factorization into prime ideals and the class field theory in algebraic number theory, as one of the development on ideas of prime numbers.

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）
class field theory （類体論）

1　序

平成21年3月に高等学校学習指導要領の改訂が行われ，数学では平成24年度より年次進行により新高等学校学習指導要領等が実施された（[Mb09] 参照）．この改訂で新たに設けられた内容として「数学A」の「整数の性質」がある．主な内容は，「約数と倍数」，「ユークリッドの互除法」，それに，整数の活用として「n 進記数法」である．本稿では，この中から特に「約数と倍数」および「ユークリッドの互除法」について，素数の性質という観点からその取り扱いにおける注意点を述べてみたい．

そのために，まず初めに教科書の内容について確認し，次に整数の性質が定義からどのように導かれているかを概観する．この過程で，素数の定義（既約元性と呼ばれる性質）を復習する．その後で，定義と命題との関係として注意すべき事項について触れ，素数の性質（素元性と呼ばれる性質）を復習する．この

＊　宮城教育大学数学教育講座

素数の既約元性と素元性という2つの性質が本稿の一つのポイントであり，この点に注意しながら，命題を証明するための手順の一例を挙げる．次に，一般的には素数のもつこの2つの性質は同値ではないことを確認する．これらが同値でないと素因数分解とその一意性は成立しない．このことを克服する一つのアイデアとしてイデアルについて復習し，素イデアル分解とその一意性への拡がりを振り返る．そして最後に，さらに深い拡がりとして，代数的整数論における類体論の概要を述べてみたい．

2 「数学A」の「整数の性質」

ここでは，平成24年1月発行の数研出版（104・数研・数A/310，[Sk12]）と平成24年2月発行の東京図書（2・東書・数A301,[Ts12]）の2つの「数学A」の教科書についてその内容を簡単に確認する．

まず章立てについては，数研出版では「図形の性質」の後の第3章に「整数の性質」があり，東京図書では「図形の性質」の前の第2章に「整数の性質」がある．各教科書の目次は次の通りである．

「数研出版：第3章　整数の性質」
第1節　約数と倍数
　1．約数と倍数
　2．最大公約数と最小公倍数
　研究．最大公約数，最小公倍数の性質
　3．整数の割り算と商および余り
　研究．自然数の積と素因数の個数
　研究．割り算の余りの性質
　発展．合同式
　問題
第2節　ユークリッドの互除法
　4．ユークリッドの互除法
　5．1次不定方程式
　問題
第3節　整数の性質の活用
　6．n進法
　7．分数と小数
　問題
演習問題

「東京図書：第2章　整数の性質」
1節　約数と倍数
　1．約数と倍数
　2．最大公約数と最小公倍数
2節　ユークリッドの互除法と不定方程式
　1．除法の性質と整数の分類
　2．ユークリッドの互除法
　3．2元1次不定方程式
　参考．1次不定方程式の整数解の
　　図形的意味
　参考．互除法の原理の証明
3節　整数の性質の活用
　1．記数法
　7．小数と分数
　参考．部屋割り論法
　練習問題
　発展．合同式
　コラム．16進法

この中で「約数と倍数」，「ユークリッドの互除法(と不定方程式)」についてみると，節での分け方やタイトル表示は多少違うものの，おおよその流れは同じである（本稿では取り上げない節である「整数の性質の活用」における「分数と小数」および「小数と分数」という両社の用語の並びの違いは面白い）．

次に，具体的に内容を見ていく．まず，「約数と倍数」についてみてみる．

（数研出版：約数と倍数）
・約数と倍数の定義
・倍数の判定法
　－2と5および4の倍数判定は証明有
　－3と9の倍数判定は4桁の整数で解説
・素数と素因数分解
　－素数の定義（既約元性による）
　－素因数分解ができることの証明有
　－素因数分解の一意性は証明無
　－約数の個数の解説

（東京図書：約数と倍数）
・約数と倍数の定義
・いろいろな数の倍数

－3の倍数判定は3桁の整数で解説
・素因数分解と約数
－素数の定義（既約元性による）
－素因数分解とその一意性は証明無

ここで，素数の定義の部分で「既約元性による」と書いたので，このことについて復習しておく．まず，素数の定義は教科書でも述べられているように次のようになる．

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．ここで，$a \mid p$ は a が p の約数であるということを表す．

この性質は，次の既約元の定義のもとになっているものであり，このことを本稿では既約元性と呼ぶ．

定義 2.2（既約元） 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，

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

を満たすこととする．

ここで，零元とは加法の単位元0のことであり，単元とは R の中で逆元をもつ元のことである．可換環として整数の全体 $\mathbb{Z}$ を考えれば，1は単元であるので，素数の定義からは外されるということになる（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，既約元の定義からわかる通り，単元の違いは積への分解において本質的ではないので，正の整数だけを考えて素数を定義している）．

次に，「最大公約数と最小公倍数」について見てみる．簡単のため，最大公約数はgcd，最小公倍数はlcmと略記し，a と b の最大公約数を$\gcd(a, b)$，最小公倍数を$\mathrm{lcm}(a, b)$ で表す．

（数研出版：最大公約数と最小公倍数）
・最大公約数と最小公倍数の定義
－「公約数｜gcd」を証明無しで紹介
－「lcm｜公倍数」を証明無しで紹介
・互いに素の定義
－「$\gcd(a, b) = 1$ のとき $b \mid ak$ ならば $b \mid k$」を証明無しで紹介
－「研究」で「$ab = \gcd(a, b)\mathrm{lcm}(a, b)$」の解説（その中で証明無しの「$\gcd(a, b) = 1$ のとき $b \mid ak$ ならば $b \mid k$」を利用）

（東京図書：最大公約数と最小公倍数）
・最大公約数の定義
・互いに素の定義
・最小公倍数の定義
－「公約数｜gcd」を証明無しで紹介
－「lcm｜公倍数」を証明無しで紹介
－「$ab = \gcd(a, b)\mathrm{lcm}(a, b)$」を具体例で例示

次に，「除法の原理（除法の性質，整数の割り算）」について見てみる．

（数研出版：整数の割り算と商および余り）
・整数の割り算（除法の原理）
－除法の原理を具体例で例示
・余りによる整数の分類

（東京図書：除法の性質と整数の分類）
・除法の性質（除法の原理）
－除法の原理を具体例で例示
・整数の分類

続いて，「ユークリッドの互除法」について見てみる．

（数研出版：ユークリッドの互除法）
・割り算と最大公約数
－互除法の原理の証明有
・ユークリッドの互除法
－互除法を具体例で明示
・最大公約数を表す式
－$ax + by = \gcd(a, b)$ が整数解をもつことを例示
－$\gcd(a, b) = 1$ のとき $ax + by = c$（c は任意）が整数解をもつことを例示

（東京図書：ユークリッドの互除法）

・互除法の原理
　－「参考」に互除法の原理の証明有
・ユークリッドの互除法
　－互除法を具体例で明示

最後に，「（２元）１次不定方程式」について見てみる．

（数研出版：１次不定方程式）
・１次不定方程式と整数解
　－ $ax + by = 0$ の整数解が無数に存在することを具体例で明示
　－$\gcd(a, b) = 1$ のとき $ax + by = c$（c は任意）の整数解の一般解を前節の例示からの結論を引用し説明
・１次不定方程式の利用

（東京図書：２元１次不定方程式）
・整数解の求め方
　－「$\gcd(a, b) = 1$ のとき $ax = by$ ならば $b \mid x$ かつ $a \mid y$」を証明無しで紹介
　－ $ax + by = 0$ の整数解が無数に存在することを解説（その中で証明無しの「$\gcd(a, b) = 1$ のとき $ax = by$ ならば $b \mid x$ かつ $a \mid y$」を利用）
・１次不定方程式の解法
　－$\gcd(a, b) = 1$ のとき $ax + by = 1$ は整数解をもつことを証明無しで紹介
・１次不定方程式とユークリッドの互除法
　－$\gcd(a, b) = 1$ のとき $ax + by = 1$ の整数解の一般解を具体例で明示

この２つの教科書では，数研出版の方が詳しく書かれているように見受けられる．しかし，そのまま鵜呑みにすると理解の上で危険な点もある．次章でこの点について説明する．

3　素因数分解を利用した命題の証明

この章では，教科書の整数の性質で取り上げられている次の命題について考えてみる．

命題 3.1　a, bを零でない整数とするとき，

$$ab = \gcd(a, b)\mathrm{lcm}(a, b)$$

が成り立つ．

この命題は，数研出版では第１節の研究としてその解説がなされ，東京図書では証明無しに具体例を通して例示されている．この数研出版の解説を眺めてみると（ここでは証明とは呼ばす，あえて解説と書いておく），その中で次の命題が使われている．

命題 3.2　$\gcd(a, b) = 1$ のとき，$ax = by$ ならば $b \mid x$ かつ $a \mid y$ である．

これは東京図書でも２元１次不定方程式の節で証明無しに登場する命題である．この命題は素因数分解のことがわかっていれば自明な命題といってよいものであり，その本質的な部分は次の命題である（素因数分解のことを利用すれば，gcdとlcmの素因数表示により命題3.1はそもそも直ちに示せる）．

命題 3.3　$\gcd(a, b) = 1$ のとき，$b \mid ak$ ならば $b \mid k$ である．

素因数分解がわかっていれば自明であると述べたが，素因数分解とその一意性はどのように示すのであろうか．分解ができることの証明は数研出版でも述べられているが，一意性についてはどちらの教科書にも触れられていない．この一意性の証明の最もポピュラーなものは次の素数の性質を利用するものである．

命題 3.4　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，素数の「素」という意味を言い表しているものであり，整数を積で分解したとき素数はどちらかの約数になっている，つまり，整数を積に細分化し続けたとき最後に残るもの（物質でいうところの元素）が素数であるということである．この性質を持つ元は，可換環 R の中では素元と呼ばれている．定義は次の通りである．

定義 3.5（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．

整数に関する問題を考える場合，素数について先の章で述べた既約元としての性質と今述べた素元としての性質を当たり前の如く利用する習慣がある．しかし，正しく理解するためには，定義からの証明が必要であろう．そこで，数論のテキストでよく見かける命題 3.4 の証明を一つ挙げてみる．

（命題 3.4 の証明 1）$p \mid a$ のとき主張は自明である．$p \nmid a$ のとき，$\gcd(a, p) = 1$ であるので，

$$p \mid ab \text{ ならば } p \mid b$$

となり，このときも主張は正しい．□

さて，ここで「あれ?」と思って頂きたい．ここで利用した性質はよく見ると命題 3.3 である．つまり，

$ab = \gcd(a, b)\mathrm{lcm}(a, b)$ を示したい
- ⇝ 命題 3.3 に帰着
- ⇝ 素因数分解とその一意性に帰着
- ⇝ 命題 3.4（素元性）に帰着
- ⇝ 命題 3.3 に帰着！

となり，トートロジーとなってしまう．これでは不味い．いくつかの専門書を頼りに証明を補完しようとすると起りそうな落とし穴であり，このまま生徒の質問に答えることは危険であろう．

もちろん，回避する方法はある．そういう点を理解して教科書を読まないとならないので，新課程で新しく登場した整数の性質は教師の側からみると本質的な部分で難しいと言える．以下，回避方法の一例をあげておく．この方法は，これまで触れていなかった，教科書では後の節で登場するユークリッドの互除法（2 元 1 次不定方程式の性質）を利用するものである．

（命題 3.4 の証明 2）ユークリッドの互除法からの帰結である次の命題を利用する．

命題 3.6 $\gcd(a, b) = 1$ ならば $ax + by = 1$ には整数解がある．

まず，$p \mid a$ のとき主張は自明であることは同じである．$p \nmid a$ のとき，$\gcd(a, p) = 1$ であるので，

$$ax + py = 1$$

を満たす整数 x, y が存在する．両辺を b 倍すると，

$$p \mid abx + pby = b$$

となり，主張が成り立つことがわかる．□

いま，命題 3.6 を利用したが，今度はトートロジーにはならないだろうか．この点は確認しておく必要があるが，きちんと機能する．本稿では細かい部分には触れず，流れだけを書くことにする．行間は高木貞治の初等整数論講義 [Ta71b] を参照して頂ければわかって頂けるはずである．

$ab = \gcd(a, b)\mathrm{lcm}(a, b)$ を示したい
- ⇝ 命題 3.3 に帰着
- ⇝ 素因数分解とその一意性に帰着
- ⇝ 命題 3.4（素元性）に帰着
- ⇝ 命題 3.6 に帰着
- ⇝ ユークリッドの互除法に帰着
- ⇝ 互除法の原理に帰着
- （⇝ 除法の原理に帰着）
- ⇝ 約数と倍数の扱いで示せる

となり，最終的に約数と倍数の定義から示せることになる（なお，[Ta71b] では約数と倍数の定義からより直接的に命題 3.1 の証明が書かれている）．

整数は初等教育段階から扱っている基本的なものであるために，その性質が「明らかである」と思われていたり，「すでにわかっていること」として利用されることがある．ここでは，取り上げなかったが，教科書で証明無しに紹介されていた

「公約数 | gcd」，「lcm | 公倍数」

の証明も手順を違えるとなかなか難しい（これらの証明は [Ta71b] で確認できる）．整数の性質が高等学校で新たに取り入れられたことを機会に，一度定義と命題の関係を確認しておくことは意義があるだろう．

4　素元と既約元および素因数分解

高等学校の新課程の「数学Ａ」で新しく登場した「整数の性質」について，素数の定義と性質に注目しながら，教科書に登場する命題について考えてきた．これまででわかったことは，素数の定義である既約元性から素数の性質である素元性が示せるということである．つまり，整数 $\mathbb{Z}$ においては，

既約元ならば素元

が成り立つ．一般に，整域（可換環で 0 以外に零因子をもたないもの）であれば，この逆である

素元ならば既約元

が成り立つことが知られている（[Ki07] 参照）．よって特に，整数 $\mathbb{Z}$ においては，素元と既約元とは同値である．つまり，実際には，どちらを定義として採用しても同じ定理が示せる．しかしながら，一般の可換環では様子が異なる．つまり，既約元と素元という概念は必ずしも一致しないのである．一つ例を挙げておこう．

例 4.1　$R=\mathbb{Z}[\sqrt{-5}]$ とする．ここで，

$$\mathbb{Z}[\sqrt{-5}]=\{a+b\sqrt{-5}\,|\,a,b\in\mathbb{Z}\}$$

である．これは普通の和と積で可換環になる（整域でもある）．$R=\mathbb{Z}[\sqrt{-5}]$ では，6 は次の 2 つの分解をもつ．

$$6 = 2\cdot 3=(1+\sqrt{-5})(1-\sqrt{-5})$$

ここで，$2, 3, 1+\sqrt{-5}, 1-\sqrt{-5}$ の 4 つの元はすべて $R=\mathbb{Z}[\sqrt{-5}]$ の既約元となることが確かめられる（つまり，これらの元の約元は ± 1 か自分自身に ± 1 を乗じた元である）．しかし，素元ではない（たとえば，2 は $1+\sqrt{-5}$ の約元でも $1-\sqrt{-5}$ の約元でもない）．よって，R における既約元であるが素元でないものが存在し，同時に R の既約元（これが整数 $\mathbb{Z}$ における素数の定義に従った対象）による分解の一意性は成り立たないことになる．

このように一般の可換環では既約元と素元の観念は必ずしも一致せず，しかも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がわかる．つまり，素数の既約元性と素元性は明確に違う性質のものであり，整数の性質に関する命題の証明において，どの役割を利用しているかを知ることは大切なことであると言えるだろう．

5　イデアルの登場

一般の可換環では，整数における素数の概念に相当する既約元について，既約元分解の一意性が成り立つとは限らないことがわかった．しかし，成り立たないから数学はそこで効力を失うかというとそうではない．この既約元分解とその一意性をある意味で回復させるのがイデアルというアイデアである．

R を可換環とし，I を R の空でない部分集合とする．

定義 5.1　I（$\neq\phi$）がRのイデアルであるとは，次を満たすこととする．

(1) $a, b\in I$ ならば $a-b\in I$（つまり，I は R の加法群としての部分群）

(2) $a\in I, r\in R$ ならば $ra\in I$

たとえば，$\{0\}$ や R 自身は R のイデアルである．また，R の元 a に対して，

$$(a)=\{ra\mid r\in R\}$$

と定めると，これも R のイデアルで，a の生成する単項イデアルと呼ばれる．R が整域であって，そのすべてのイデアルが単項イデアルであるとき，R を単項イデアル整域（PIDとしばしば略記）という．単項イデアル整域では次のことが成り立つ（[Ki07]参照）．

命題 5.2　単項イデアル整域では，既約元であることと素元であることは同値である．

これによって，特に整数の成す環（整域）$\mathbb{Z}$ では 2 つの素数の性質である既約元性と素元性が同値となる．

さて，例 4.1 の可換環 $R=\mathbb{Z}[\sqrt{-5}]$ では既約元と素元が同値ではなかったため，$R=\mathbb{Z}[\sqrt{-5}]$ はPID ではないということがわかる．実際に，たとえば $R=\mathbb{Z}[\sqrt{-5}]$ の 2 つの元 α,β に対して，

$$(\alpha,\beta)=\{r\alpha+s\beta\mid r,s\in R\}$$

とおくと，これは $R=\mathbb{Z}[\sqrt{-5}]$ のイデアルとなるが，

$$\mathfrak{p}_1 = (2, 1 + \sqrt{-5}),$$
$$\mathfrak{p}_2 = (2, 1 - \sqrt{-5}),$$
$$\mathfrak{q}_1 = (3, 1 + \sqrt{-5}),$$
$$\mathfrak{q}_2 = (3, 1 - \sqrt{-5})$$

はいずれも単項イデアルではないことが確かめられる．R の 2 つのイデアル I, J に対して，その積 IJ を I の元 α と J の元 β の積 $\alpha\beta$ をすべて含むような R のイデアルとする．このとき，$\mathfrak{p}_1 = \mathfrak{p}_2$ であり，

$$\mathfrak{p}_1^2 = (2),$$
$$\mathfrak{q}_1\mathfrak{q}_2 = (3),$$
$$\mathfrak{p}_1\mathfrak{q}_1 = (1 + \sqrt{-5}),$$
$$\mathfrak{p}_2\mathfrak{q}_2 = (1 - \sqrt{-5}),$$

となるので，イデアルというレベルで考えると，$6 = 2 \cdot 3$ という分解も $6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ という分解も

$$(6) = \mathfrak{p}_1^2\mathfrak{q}_1\mathfrak{q}_2 \qquad (1)$$

と同じタイプの分解に落ち着く．そこで，イデアルに対して素イデアルを次のように定義する．

定義 5.3 R を可換環とする．R のイデアル P が素イデアルであるとは，$a, b \in R$ に対して

$$ab \in P \text{ ならば } a \in P \text{ または } b \in P$$

を満たすこととする．

この定義から，I が 0 でも単元でもない元 p で生成される単項イデアル (p) であるとき，(p) が素イデアルであることと p が素元であることは同値であることがわかる（$a \in (p)$ とは $p \mid a$ ということである）ので，素イデアルは素元という概念のイデアル版と言える．

上で登場した $R = \mathbb{Z}[\sqrt{-5}]$ のイデアル $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{q}_1, \mathfrak{q}_2$ はいずれも素イデアルであることが確かめられるので，式(1) はイデアルのレベルで考えると，素イデアルの積に一意的に分解できることを暗示している．つまり，$R = \mathbb{Z}[\sqrt{-5}]$ では既約元分解は成立しないのであるが，イデアルという概念を導入し，素イデアルの積に分解することで，その一意性が（ここでは単項イデアル (6) だけの考察であるが）回復されたわけである．一般的には，次のような定理が知られている（[Ad10] または [Ki07] 参照）．

定理 5.4（素イデアル分解とその一意性） R をデデキント整域とする．ここで，デデキント整域とは，

(1) イデアルの任意の増大列は有限で止まる（ネーター性），

(2) R の商体 K の元であって係数が R のモニック多項式の根は R の元に限る（整閉性），

(3) R の零でないすべての素イデアルは極大イデアルである．

を満たす整域である．このとき，R の零でも R 自身でもないイデアル I は

$$I = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_r^{e_r}, \quad \mathfrak{p}_i \text{ は素イデアル}$$

と素イデアルの積に分解でき，その分解は素イデアルの順序を除いて一意的である．ここで，e_i と r は自然数である．

このように，既約元分解が崩壊する環においても，見方を拡げると素イデアル分解という形で一意性が回復できる．また，整数の成す環 $\mathbb{Z}$ は PID かつデデキント整域であるので，数とイデアルを対応させることによって，上の定理は整数 $\mathbb{Z}$ における素因数分解とその一意性定理の一般化であると見てとれる．

6　イデアル類群と類体論

有理数体 $\mathbb{Q}$ 上の代数的な複素数，つまり，有理数係数の多項式の根となる複素数を代数的数という．また，その中で特に，整数 $\mathbb{Z}$ を係数にもつモニック多項式の根となる複素数を代数的整数という．代数的数は体になるが，その部分体を代数体と呼び，特に $\mathbb{Q}$ 上のベクトル空間としての次元が有限である代数体を有限次代数体と呼ぶ（以下，本章の内容の詳細は [Ad10]，[Ka92] または [Ta71a] を参照のこと）．

k を有限次拡大体とする．O_k を k に含まれる代数的整数の全体とし，これを k の整数環と呼ぶ．たとえば，

$$k = \mathbb{Q}(\sqrt{-5}) = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Q}\}$$

は $\mathbb{Q}$ 上 2 次の代数体であり，

$$O_k = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$$

はその整数環である．整数環はデデキント整域であるので，先の章で述べた素イデアル分解とその一意性の定理が成り立つ．

有限次代数体 k の部分集合 I が O_k 加群であり，さらに，O_k の零でない元 d で $dI \in O_k$ となるものが存

在するとき，この I を k の分数イデアルという．I_k で k の分数イデアルの全体を表し，P_k でその中で単項イデアルであるものの全体を表す．このとき，I_k はイデアルの積でアーベル群となり，P_k はその部分群である．そこで，その商群 I_k/P_k を C_k で表し，k のイデアル類群と呼ぶ．単項イデアル整域では既約元分解（つまり素元分解）とその一意性が成り立ったので（[Ki07] 参照），イデアル類群は素元分解の困難さを表す構造物とみなすことが出来る．さらに，このイデアル類群は有限であるという著しい性質をもつ．

さて，$R=\mathbb{Z}[\sqrt{-5}]$ では素イデアル分解とその一意性が成り立つわけであるが，その分解の様子はガロア拡大 $\mathbb{Q}(\sqrt{-5})/\mathbb{Q}$ のガロア群 $\mathrm{Gal}(\mathbb{Q}(\sqrt{-5})/\mathbb{Q})$ を通してわかる．つまり，$\mathbb{Z}$ の素数 p に対して，法 p における平方剰余記号 $\left(\frac{-5}{p}\right)$ を対応させてできる写像

$$\begin{array}{ccc}\sigma:\mathbb{Z}\setminus\{2,5\} & \longrightarrow & \mathrm{Gal}(\mathbb{Q}(\sqrt{-5})/\mathbb{Q}) \\ \cup & & \cup \\ p & \longmapsto & \left(\frac{-5}{p}\right)\end{array}$$

を通して，

$$\begin{cases}\sigma(p)=1 & \Leftrightarrow\ (p)=\mathfrak{p}\mathfrak{p}'\text{：分解} \\ \sigma(p)=-1 & \Leftrightarrow\ (p)\text{：素イデアルのまま}\end{cases}$$

が成り立つことがわかる（ここで除外されている $p=2,5$ は k において素イデアルの 2 乗になる）．ここで，平方剰余記号は，

$$\left(\frac{-5}{p}\right)=\begin{cases}1 & p\equiv 1,3,7,9\ (\mathrm{mod}\ 20) \\ -1 & p\equiv 11,13,17,19\ (\mathrm{mod}\ 20)\end{cases}$$

である．

一般に，与えられた代数体 k で次の性質をもつガロア拡大体 $\tilde{k}$ が存在するであろう，というのが Hilbert が提起した予想である．

「$\tilde{k}/k$の拡大次数を n とするとき，k の素イデアルが $\tilde{k}$ で単項イデアルとなるとき，かつ，その場合に限って，$\tilde{k}$ において完全分解（つまり，n 個の素イデアルの積に分解）する」

このような代数体 $\tilde{k}$ を k の絶対類体（Hilbert 類体）という．この予想は Furtwänger によって肯定的に解決され，絶対類体 $\tilde{k}$ は常に存在し，次が成り立つことが知られている．

(1) $\tilde{k}$ は唯一つである．

(2) $\tilde{k}/k$ はアーベル拡大体であり，次が成り立つ．

$$C_k\simeq\mathrm{Gal}(\tilde{k}/k)$$

(3) $\tilde{k}/k$ は不分岐拡大である（つまり，冪の形に分解する素イデアルはない）．

(4) k の素イデアル $\mathfrak{p}$ は，$\mathfrak{p}^f$ が単項イデアルとなる最小の自然数 f を取ると，$\tilde{k}$ において次のように素イデアル分解される．

$$\mathfrak{p}=\mathfrak{P}_1\cdots\mathfrak{P}_g,\quad fg=[\tilde{k}:k]$$

これが類体論の最も基本的な命題である．これは更に，無限素点を込めたイデアルを法とする合同を利用することにより一般化されている．以下，大まかに概要を述べる．

k を有限次代数体，$\mathfrak{m}$ を k のイデアル（いわゆる無限素点も込めたイデアル）とし，$I_k(\mathfrak{m})$ で $\mathfrak{m}$ の有限素点部分と素（因子無縁）な k の分数イデアル全体のなす群を表し，また，$I_k(\mathfrak{m})$ の部分群 $S_k(\mathfrak{m})$ を

$$S_k(\mathfrak{m})=\{(\alpha)\in P_k\mid \alpha\equiv 1\ (\mathrm{mod}\ \mathfrak{m})\}$$

によって定める．ここで，イデアルを法とした合同式は無限素点も含めた合同である．このとき，商群 $I_k(\mathfrak{m})/S_k(\mathfrak{m})$ を $C_k(\mathfrak{m})$で表し，k の法 $\mathfrak{m}$ のイデアル類群と呼ぶ．$\mathfrak{m}=(1)$ のときには $C_k(\mathfrak{m})=C_k$ である．

$C_k(\mathfrak{m})$の部分群 $H_k(\mathfrak{m})$に対して，拡大体 K/k が$H_k(\mathfrak{m})$の類体であるとは，次を満たすこととする．

「K/k はガロア拡大であって，
$\mathfrak{m}$ と素な k のイデアル $\mathfrak{p}$ は，
$\mathfrak{p}S_k(\mathfrak{m})\in H_k(\mathfrak{m})$ となるとき，
かつ，その場合に限って，K において完全分解（つまり，拡大次数と同じ個数の素イデアルの積に分解）する．」

この類体の存在を示したのが次の主定理を含む「高木の類体論」である．

定理 6.1　次が成り立つ．

(1) アーベル拡大 K/k は，あるイデアル $\mathfrak{m}$ に関する$H_k(\mathfrak{m})$ の類体である．ここで，$\mathfrak{m}$ は K/k で分岐する（冪の形に分解する）素イデアルのみを含む．

(2) 任意の $H_k(\mathfrak{m})$ に対して，その類体は唯一つである．

(3) K を $H_k(\mathfrak{m})$ の類体とするとき，次が成り立つ．

$$C_k(\mathfrak{m})/H_k(\mathfrak{m})\simeq\mathrm{Gal}(K/k)$$

(4) k の素イデアル $\mathfrak{p}\in I_k(\mathfrak{m})$ は，$\mathfrak{p}\in S_k(\mathfrak{m})\in H_K(\mathfrak{m})$ と

なる最小の自然数 f を取ると，K において次のように素イデアル分解される．

$$\mathfrak{p} = \mathfrak{P}_1 \cdots \mathfrak{P}_g, \quad fg = [K : k]$$

たとえば，既約元分解の一意性が成り立たない整数環 $\mathbb{Z}[\sqrt{-5}]$ をもつ 2 次の代数体 $\mathbb{Q}(\sqrt{-5})$ について具体的に書いてみると，法(20) のイデアル類群の剰余群と $\mathbb{Q}(\sqrt{-5})$ の $\mathbb{Q}$ 上のガロア群との間に

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

となる同型がある．先の例 4.1 では，(2)が分岐し，(3)が完全分解していることを具体的な計算によって示したが，この定理を用いれば，2 は20の約数であるのでイデアル(2)は分岐し（定理 6.1 の(1)），イデアル(3)の類は $H_{\mathbb{Q}}((20))$ の元なのでイデアル(3)は完全分解していることがわかる（定理 6.1 の(4)）．これによって，イデアル(6)は $\mathbb{Q}(\sqrt{-5})$ において，相異なる素イデアル $\mathfrak{p}, \mathfrak{q}, \mathfrak{q}'$ を用いて

$$(6) = \mathfrak{p}^2\mathfrak{q}\mathfrak{q}'$$

と分解できることがわかるのである．

7　まとめ

本稿では，新課程「数学Ａ」で新しく導入された「整数の性質」のうち，「約数と倍数」および「ユークリッドの互除法（と１次不定方程式）」で取り上げられている内容を確認し，特に，素数に注目して，命題の理解において注意すべき点を述べてみた．その素数の性質とは，既約元としての性質と素元としての性質である．これらは一般的には同値な概念ではないが，整数の成す環 $\mathbb{Z}$ では同値になる．$\mathbb{Z}$ における同値性は証明のないまま，初等教育課程から利用されており，素因数分解とその一意性を利用するときには当たり前（自明であると良く言う）で通り過ぎることになる．しかし，一般の可換環では，既約元と素元とが一致しないために，既約元分解の一意性が成り立たないことがある．素数の定義は既約元としての性質に基づいていたので，これは素因数分解の一意性が成り立たないことがあることを意味する．その「成り立たない度合」を表したものがイデアル類群であり，イデアルという概念を用いると，この崩壊していた既約元分解とその一意性を素イデアル分解とその一意性という形で回復できることがある．代数体 k の整数環 O_k はまさに素イデアル分解の導入により，その分解と一意性が回復できる代表的な例である．イデアル類群という既約元分解の難しさを表す量と回復された素イデアル分解の具体的な分解の様子は，類体論を通して，２つの代数体の間で互いに繋がっている．

このような数学の拡がりを通して，改めて「整数の性質」を眺めてみると，人の営みの偉大さが実感できることと思う．

参考文献

[Ad10] 足立恒雄, 改訂新版　類体論へ至る道　初等数論から代数入門, 日本評論社, 2010年 2 月.
[Ka92] 河田敬義，数論－古典数論から類体論へ－，岩波書店，1992年 4 月.
[Ki07] 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.
[Sk12] 数学Ａ, 数研出版，平成24年 1 月.
[Ta71a] 高木貞治, 代数的整数論　第 2 版，岩波書店, 1971年 4 月.
[Ta71b] 高木貞治, 初等整数論講義　第 2 版，共立出版, 1971年 10 月.
[Ts12] 数学Ａ, 東京図書，平成24年 2 月.
[Mb09] 文部科学省, 高等学校学習指導要領解説, 平成21年12月.

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27年 9 月30日受理）