第1章　序

1.1　フェルマーの最終定理

ピタゴラスの定理（三平方の定理）は古くから知られている．

定理 1.1 直角３角形の直角をはさむ２辺の長さを a, b とし，他の１辺の長さを c とすれば，

$$a^2 + b^2 = c^2$$

が成り立つ．

そこで，長さが整数である直角３角形を作るには，方程式 $x^2 + y^2 = z^2$ （これを**ピタゴラス方程式**という）の整数解を求めればよい． この整数解についても古くから知られていたようである．

定理 1.2 方程式

$$x^2 + y^2 = z^2$$

の自然数解は，$u > v$ をみたす自然数 u, v をとって

$$x = u^2 - v^2, \quad y = 2uv, \quad z = u^2 + v^2$$

または，

$$x = 2uv, \quad y = u^2 - v^2, \quad z = u^2 + v^2$$

とおくことによってすべて得られる．

証明は，いつかどこかで....
たとえば，$u = 2, v = 1$ あるいは $u = 3, v = 2$ とすれば，

$$(x, y, z) = (2^2 - 1^1, 2 \cdot 2 \cdot 1, 2^2 + 1^2) = (3, 4, 5)$$
$$(x, y, z) = (3^2 - 2^2, 2 \cdot 3 \cdot 2, 3^2 + 2^2) = (5, 12, 13)$$

というよく知られた解が得られるし，$u = 1957, v = 54$ をとれば，

$$(x, y, z) = (3826933, 211356, 3832765)$$

というあまり知られていない（っていうかほとんどの人が知らない）解も出てくる．

さて，ピタゴラス方程式は 2 次式で表されているが，これを 3 次にするとどうなるか？フェルマー（17 世紀の人）は，そのような方程式には自然数解がなく，さらに 4 次以上でも同様に自然数解がないことを「証明」したが，その証明は残されていない．

定理 1.3 (フェルマーの最終定理) 自然数 $n \geq 3$ に対して，方程式

$$x^n + y^n = z^n$$

は自然数解をもたない．

この定理は，長い間証明が知られていなかったので，かつては『フェルマー予想』とも呼ばれ，整数論における難問のひとつであった． フェルマー自身によって $n = 4$ の場合が証明され，$n = 3$ に対してはオイラーが証明を与えている（それぞれ、17，18 世紀）． その後，ソフィ・ジェルマン，ラメ，クンマー等による貢献があったが，20 世紀になって整数論や代数幾何学の理論が少しずつ整えられた結果，1994 年ワイルズによって完全な証明が与えられた． その証明は数多くの高度な理論を駆使して構成され，大胆な発想に満ちている． ちょうど，中島匠一先生による解説講演があるので是非お聴きなさい (2011 年 10 月 1 日 14:45–15:55 於 南 7–101).

1.2　未解決問題

一般に数学の問題は難しい概念を用いて語られ，専門に学んだ人でなければ問題を理解することすら困難であることが多い． しかし，整数論の問題は初等的に表現されるものもあり，それらの多くは中高生でも（もしかすると小学生でも）理解できる． 前述の『フェルマーの最終定理（フェルマー予想)』もそんな類の問題であった． 他にもいくつかあるので思いつくままに列挙してみる．

完全数の問題 【未解決】その数より小さい約数の和がその数になるとき完全数という．$2^n - 1$ が素数のとき $2^{n-1}(2^n - 1)$ が完全数となることは古代から知られていた． さらにオイラーによって，偶数の完全数は必ずこのように表されることも証明されている． 偶数の完全数は無限個あるか？　また，奇数の完全数は存在するか？

コラッツの問題 【未解決】自然数 x が偶数ならば $x/2$ とし，奇数ならば $3x + 1$ とする操作を考える． すべての自然数は，この操作を繰り返しほどこすことで必ず 1 になるか？ たとえば 6 から始めてこの操作を繰り返しほどこすと，$6 \to 3 \to 10 \to 5 \to 16 \to 8 \to 4 \to 2 \to 1$ となる．

合同数の問題 【未解決】3 辺の長さが有理数である直角 3 角形の面積となる有理数を合同数という． 自然数 n が合同数となるための条件を見つけよ． この問題は，方程式 $y^2 = x^3 - n^2 x$ の有理数解と密接な関わりがあり，さらに楕円曲線論の『バーチ・ス

ウィンナートン＝ダイアー予想』とも関連する． この予想の証明（または反証）は，100 万ドルの賞金がかかった問題（ミレニアム懸賞問題）のひとつで未解決のままである．

双子素数予想 【未解決】差が 2 である素数の組を双子素数という． 双子素数は無限組存在する．

ゴールドバッハ予想 【未解決】6 以上の任意の偶数は 2 つの素数の和として表すことができる．

カタラン予想 $x^a - y^b = 1$ をみたす 1 より大きい自然数 x, a, y, b の組は $(x, a, y, b) = (3, 2, 2, 3)$ のみである． 2003 年にミハイレスクによって証明された．

1.3 集合の記法 (復習)

いくつかのものをひとまとめにして考えた “ものの集まり” を**集合**という． 集合はふつう大文字で表される． 集合 A の中に入っている個々の ‘もの’ を，A の**元** (または**要素**) という． a が A の元であることを

$$a \in A$$

で表す． また，$a \in A$ でないことを $a \notin A$ で表す． 集合 A と ‘もの’ a が与えられたとき，$a \in A$ であるかそうでないかがはっきりと定まっていなければならない． $a \in A$ でありかつ $a \notin A$ であったり，どちらも成り立たないというようなことはない． 必ず，$a \in A$, $a \notin A$ のどちらか一方が成り立つ．

集合 A はその元により定まるが，元が $a, b, c, \cdots$ のようにはっきりと明示できるとき，

$$A = \{a, b, c, \cdots\}$$

のように書く． たとえば，4 つの自然数 $2, 3, 6, 11$ のみを元とする集合（これを $2, 3, 6, 11$ からなる集合ということがある）は

$$\{2, 3, 6, 11\}$$

である． 元の順序は無視され，また重ねて表示することも禁止されないから，

$$\{2, 3, 6, 11\} = \{3, 11, 2, 6\} = \{2, 3, 2, 11, 11, 6, 11, 2\}$$

である． 元をひとつももたない集合も考え，それを ϕ で表し**空集合**という． 空集合は $\{\ \}$ と表すことができる．

$$\phi = \{\ \}.$$

自然数全体，整数全体の集合 $\boldsymbol{N}$，$\boldsymbol{Z}$ は，

$$\boldsymbol{N} = \{1, 2, 3, \cdots\}, \quad \boldsymbol{Z} = \{\cdots, -3, -2, -1, 0, 1, 2, 3, \cdots\}$$

と書ける． ここで，‘$\cdots$’ で表された部分が容易に推察できることが前提となっていることに注意すべきである． たとえば，

$$A = \{2, 4, 6, 8, \cdots\}, \quad B = \{2, 3, 5, 7, \cdots\}$$

において， A は正の偶数全体の集合であることが推察できるが，B の ‘$\cdots$’ が何を意味するかは少し曖昧である． 話題が整数論ならば，B は素数全体の集合と解釈できるかもしれないが，それとは別に，数列

$$b_n = \frac{-n^3 + 9n^2 - 14n + 18}{6}$$

の作る集合とみることもできる． 実際，$\{b_n\}_{n=1,2,\cdots}$ を順に計算してみると

$$2,\ 3,\ 5,\ 7,\ 8,\ 7,\ 3,\ -5,\ -18,\ \cdots$$

となっている． このように ‘$\cdots$’ を含む記法は曖昧さを含んでいて，たとえば，A についても，数列

$$a_n = 2^n - \frac{n(n-1)(n-2)}{3}, \qquad a'_n = \frac{-n^4 + 10n^3 - 35n^2 + 54n - 24}{2}$$

いずれかの作る集合かもしれない，というように ‘$\cdots$’ をどのようにでも解釈できてしまう． したがって，‘$\cdots$’ の意味するところが文脈からはっきりと定まる場合にのみ使われるべきである．

いずれにしろ，$\{a, b, c, \cdots\}$ の形の記法は，集合の元をすべて書き上げている（あるいはその代表的な元を提示することで残りの元すべてを ‘$\cdots$’ によって類推できる）という点で，きわめてわかりやすい． しかし，すべての元をもらさずに書き並べることができない集合（たとえば，無理数全体の集合）については，曖昧さを含まずに表記するために別の記法を与える必要がある． そのために，‘もの’ についての性質というものを考える． たとえば，‘x は無理数である’ とか ‘x は平方数でない自然数である’ などは，‘もの’ x についての性質である． このような性質のひとつ $P(x)$ を考え，$P(x)$ が成り立つような x 全体の集合を

$$\{x \mid P(x)\}$$

と書く． たとえば，

$$\{x \mid x \text{ は } 1 \text{ より大きく } 7 \text{ 以下の奇数である }\}$$

は $\{3, 5, 7\}$ と等しい．

$$\{x \mid x \text{ は } 1 \text{ より大きく } 7 \text{ 以下の無理数である }\}$$

はすべての元を書き上げることはできないが，確かにひとつの集合を定める． また，有理数全体，実数全体の集合 $\boldsymbol{Q}$，$\boldsymbol{R}$ は

$$\boldsymbol{Q} = \{x \mid x \text{ は有理数 }\}, \quad \boldsymbol{R} = \{x \mid x \text{ は実数 }\}$$

で与えることができるが，もちろんこれは ‘良い’ 表し方ではない．

$$\boldsymbol{Q} = \{x \mid x \text{ は整数の商 }\}, \quad \boldsymbol{R} = \{x \mid x \text{ はコーシー列である有理数列の極限値 }\}$$

とすればより正確になる． $\boldsymbol{Q}, \boldsymbol{R}$ の厳密な定義については別の機会に論ずることにする．

さて，このような記法では，あらかじめ ‘もの’ x の動く範囲を定めておいて，その範囲の中で性質 $P(x)$ が成り立つものを集めるようにすれば，曖昧さが少なくかつ簡便に記述できる． たとえば，上にあげた ‘1 より大きく 7 以下の無理数’ 全体の集合は

$$\{x \mid x \in \boldsymbol{R} \text{ かつ } x \text{ は } 1 \text{ より大きく } 7 \text{ 以下の無理数 }\}$$

とすれば，より正確である． これを

$$\{x \in \boldsymbol{R} \mid x \text{ は } 1 \text{ より大きく } 7 \text{ 以下の無理数 }\}$$

と略記する． 無理数である実数全体の集合は

$$\{x \in \boldsymbol{R} \mid x \notin \boldsymbol{Q}\}$$

と書くことができる．

‘もの’ x がある範囲を動くとき，x の式によって表現されるもの全体の集合を考えたいときがある． たとえば，x が $\boldsymbol{Z}$ の中を動くときに，式 $2x$ で表されるもの全体が偶数全体の集合を与える． 性質 $P(x)$ をみたすような ‘もの’ x 全体について，x の式 $f(x)$ で表される ‘もの’ 全体の集合を

$$\{f(x) \mid P(x)\}$$

で表す． たとえば

$$\{2x \mid x \in \boldsymbol{Z}\}, \quad \{2y+1 \mid y \in \boldsymbol{Z}\}, \quad \{n^2 \mid n \in \boldsymbol{N}\}$$

はそれぞれ偶数全体，奇数全体、平方数全体の集合である． この記法を使えば，

$$\boldsymbol{Z} = \{a - b \mid a, b \in \boldsymbol{N}\}, \quad \boldsymbol{Q} = \left\{ \frac{a}{b} \;\middle|\; a \in \boldsymbol{Z} \text{ かつ } b \in \boldsymbol{N} \right\}$$

と書け，さらに実数全体，複素数全体の集合も

$$\boldsymbol{R} = \left\{ \lim_{n\to\infty} a_n \;\middle|\; \{a_n\} \text{ はコーシー列である有理数列} \right\},$$

$$\boldsymbol{C} = \{a + bi \mid a, b \in \boldsymbol{R}\}$$

と書くことができる． ただし i は虚数単位である．

1.4 集合の演算 (復習)

【包含関係】 ふたつの集合 A，B はその属する元がまったく同じであるとき等しい，すなわち $A = B$ となる． A が B に含まれるとき，A は B の**部分集合**であるといい

$$A \subset B$$

で表す． 正確には，$A \subset B$ とは，A に属する元がすべて B に属することである．

$$A \subset B \iff 「x \in A \text{ ならば } x \in B」.$$

$A = B$ とは，どんな‘もの’x に対しても $x \in A$ と $x \in B$ が同値となることだから，

$$A = B \iff 「A \subset B \text{ かつ } B \subset A」$$

が成り立つ (むしろ，これを $A = B$ の定義とするのが普通である).
一般に，命題（性質） $P,\ Q$ について，

$$P \text{ ならば } Q$$

であることと

$$P \text{ でないかまたは } Q$$

であることは同じことである． たとえば,「代数入門の単位を取れば進級できる」ということは,「代数入門の単位を落とすか，または進級できる」ということとまったく同じである．いま，空集合 ϕ はひとつも元をもたないから，どんな x についても $x \notin \phi$ である． よって，任意の集合 A について ($x \in A$ か $x \notin A$ にかかわらず)

$$x \in \phi \text{ でないかまたは } x \in A$$

が成り立っている． したがって，上に述べたとおり

$$x \in \phi \text{ ならば } x \in A$$

であり，これは

$$\phi \subset A$$

を意味する． すなわち，どんな集合も空集合を部分集合としてもつことがわかる．

【和集合・共通部分・差集合】 集合 A, B のそれぞれの元をすべて寄せ集めて得られる集合を A, B の**和集合**といい，$A \cup B$ で表す． 正確な定義は以下の通り;

$$A \cup B = \{x \mid x \in A \text{ または } x \in B\}.$$

一方，A, B の両方共に属する元全体の集合を A, B の**共通部分** (または**積集合**) といい，$A \cap B$ で表す.

$$A \cap B = \{x \mid x \in A \text{ かつ } x \in B\}.$$

3つ以上の集合 $A_1, A_2, \cdots, A_n$ に対しても

$$A_1 \cup A_2 \cup \cdots \cup A_n = \{x \mid \text{ある } 1 \leq i \leq n \text{ について } x \in A_i\}$$
$$A_1 \cap A_2 \cap \cdots \cap A_n = \{x \mid \text{すべての } 1 \leq i \leq n \text{ に対して } x \in A_i\}$$

によって和集合，共通部分を定める． それぞれ，

$$\bigcup_{i=1}^{n} A_i, \quad \bigcap_{i=1}^{n} A_i$$

と書くこともできる．

無限個の集合 $A_1, A_2, \cdots, A_n, \cdots$ に対してもまったく同様にして

$$\bigcup_{n=1}^{\infty} A_n = \{x \mid \text{ある } n \text{ について } x \in A_n\}$$
$$\bigcap_{n=1}^{\infty} A_n = \{x \mid \text{すべての } n \text{ に対して } x \in A_n\}$$

によって和集合，共通部分を定めることができる．

ふたつの集合 A, B に対して，A に属し B に属さない元全体の集合を A, B の差集合といい $A - B$ で表す．

$$A - B = \{x \mid x \in A \text{ かつ } x \notin B\}.$$

さて，和集合，共通部分＝積集合，差集合を上で定義したが，和・積・差があるならば商があると思ってもおかしくはない． 実際に**商集合**という概念があり，大学での数学を学ぶ上で大変重要なものとなっている． 本講義ではとくに代数的構造から定まる商集合の理解がひとつの大きな目標となる． これについては後に論ずることにする．