

はじめに

○ ピークを目指そう

この本は、

「一般の5次方程式が根号で解けないことのきちんとした証明を

いちばんやさしい筋道で理解し感得する」

ことを目指しています。

●ガロア理論の啓蒙書を読んだけど、最後の方の5次方程式が根号で解けないところの説明・証明がクリアにはわからない。

●そこで、専門書を手に取ってみたが挫折した。

●でもやはり、5次方程式が根号で解けないことの証明が気になるので読んでみたい。

このような読者の方のために、この本を書かせていただきました。

5次方程式が根号で解けないことを示すには、次の定理を証明しなければなりません。

ピークの定理

方程式 $f(x) = 0$ の解が根号で表せる

$\Leftrightarrow$ 方程式 $f(x) = 0$ のガロア群が可解群である

この定理が証明されれば、5次方程式が根号で解けないことを示すことができるのです。ガロア群も可解群も説明していないのに、いきなり専門用語を出してしまって恐縮です。

この本では、この定理を「ピークの定理」と称し、本全体を通して目標とする定理としています。

ここでいう「目標とする」という意味は、単に定理の内容を理解するだけに留まりません。定理を証明して感得するという意味です。

この本のすべての記述、定義・定理の積み重ねは、「ピークの定理」を証明するためにあるといっても過言ではありません。ですから、啓蒙書でよくあるようなガロアの人物・伝記については一言も触れていません。この手の解説は他書にお任せいたします。

「ピーク」とは山の頂の「ピーク」という意味で、この本だけの用語です。この本は、このピークの定理に登頂することを目指すアルピニストのための本なのです。

ロープウェイで途中の山小屋まで行って、頂上を眺めながらコーヒーを飲むだけでもそれは素晴らしい登山体験ですが、本書では、そのはるか先に仰ぎ見える頂上まで、一步一步、自分の力で登っていきます。

とはいえ、ハーケンを一本一本岩崖に打ちつけながらの本格的な登山スタイルで登るのでは負担が大きすぎます。そのためには資金も時間も普段からの専門的なトレーニングも必要になってきます。

そこで本書は、ピークを踏むために、もっとも体に負担の少ないルートを選びました。本書がとるルートでは、登山道には木の階段が整備してありますし、岩場には頑丈な鎖がつけてあります。必要とする装備も最小限に留めました。一步一步着実に登り続けられれば、必ずやピークを踏み、ガロア理論の全貌を眼下に見ることができるでしょう。

ここで、本書の特徴について述べておきましょう。

○ 本書の特徴

1. 証明がこの本に全部書いてある

啓蒙書の多くは、定理とその説明だけが書いてあり、証明は易しいものだけにつけてあります。

専門書には、定理の事実だけでなく証明まで記述されているのが建前です。が、専門書であっても、そこに載っている定理のすべてに証明が付けられているとは限りません。

専門書に扱われている定理の中には、定理の紹介はあっても証明は他書に譲るとしているものも多いのが現状です。これは、ピークの定理を証明するには広い範囲の分野における定理を積み重ねていかななくてはならないからだと考えられます。例えば、線形代数の基本的事項を用いるものに関しては線形代数の本を見よ、という姿勢をとっている場合が多いです。本書では、読者が線形代数の知識を知らないものとし、必要な線形代数の知識はその場で解説していきます。

また、専門書の中には、定理の証明を練習問題の形にして読者に委ねている箇所も多くあります。簡単な証明であれば読者が自力で証明を付けることができるでしょうが、初学者には無理であると思われるような命題でも練習問題にしている場合が多々あります。専門書は数学科の学生を読者として想定しているせいか、読者に要求するレベルが高すぎるわけです。

この本でも「問」を掲げて説明を進めることがありますが、それは読者に問題を解いてもらうことを想定して「問」を立てているのではありません。話を進めていく上で、テーマを明確に意識してもらうために「問」を立てているだけのことです。いわばレトリックです。本書に掲げられている「問」は、すぐそのあとに解説が続きます。解かずにそのまま読み進めていってもらうことを前提にしています。

この本の特徴は、定理が出てきた場合必ずそれをこの本の中で証明していることです。証明を他の本に投げるようなことはしていません。執念深

くすべての定理に証明が付けてあります。

正確にいうと実例をあげることで証明の代わりにしている場合も多いのですが、それは一般的な記号で書くよりも実例をあげたほうが、証明の内容を手にとるように伝えることができると考えているからです。多くは実例での数値を文字で置き換えれば、そのまま証明になります。

2. 初めから終わりまで同じ丁寧さ

啓蒙書では1から5段階までを説明するとき、初めの1, 2段階は丁寧に説明するものの、3段階になると少し論理が飛びがちになり、4段階になると言葉だけの説明になり、5段階になると結論だけを語るということになりがちです。啓蒙書を読んだ方で、後半の部分も同じ丁寧さで語ってくれたら理論全体がよく分かるのになあ、という感想を持った方も多くいらっしゃると思います。

この本では、初めのとっつきからピークの定理まで、同じ丁寧さで解説をすることを心がけました。特に、ガロア対応の証明や「ピークの定理」の証明は、他の啓蒙書にはない丁寧さになっていると思います。

3. 例から説明している

多くの専門書では、定義・定理を述べてからその実例を示し理解を促します。実例を示してあればいい方で、示されない場合も多々あります。数学の専門書は抽象的で読みづらいのです。

本書では、まず例を示し、それから定義・定理を述べていく説明の順序をとっています。抽象的な専門書でつまづいた人でも、本書なら読み進めていくことができるはずです。

4. 高校数学を履修した人であれば読める

本書では、高校で履修した数学こそ前提の知識としますが、それ以外の項目は習っていないものとして解説を進めます。

複素数についても定義から始めて解説してあります。複素数は文部科学省のカリキュラム変更によって、履修項目に含まれたり外されたりを繰り返した単元で、読者の年代により複素数に対する理解度がまちまちであると考えられるからです。

5. 一番易しいルートを選択

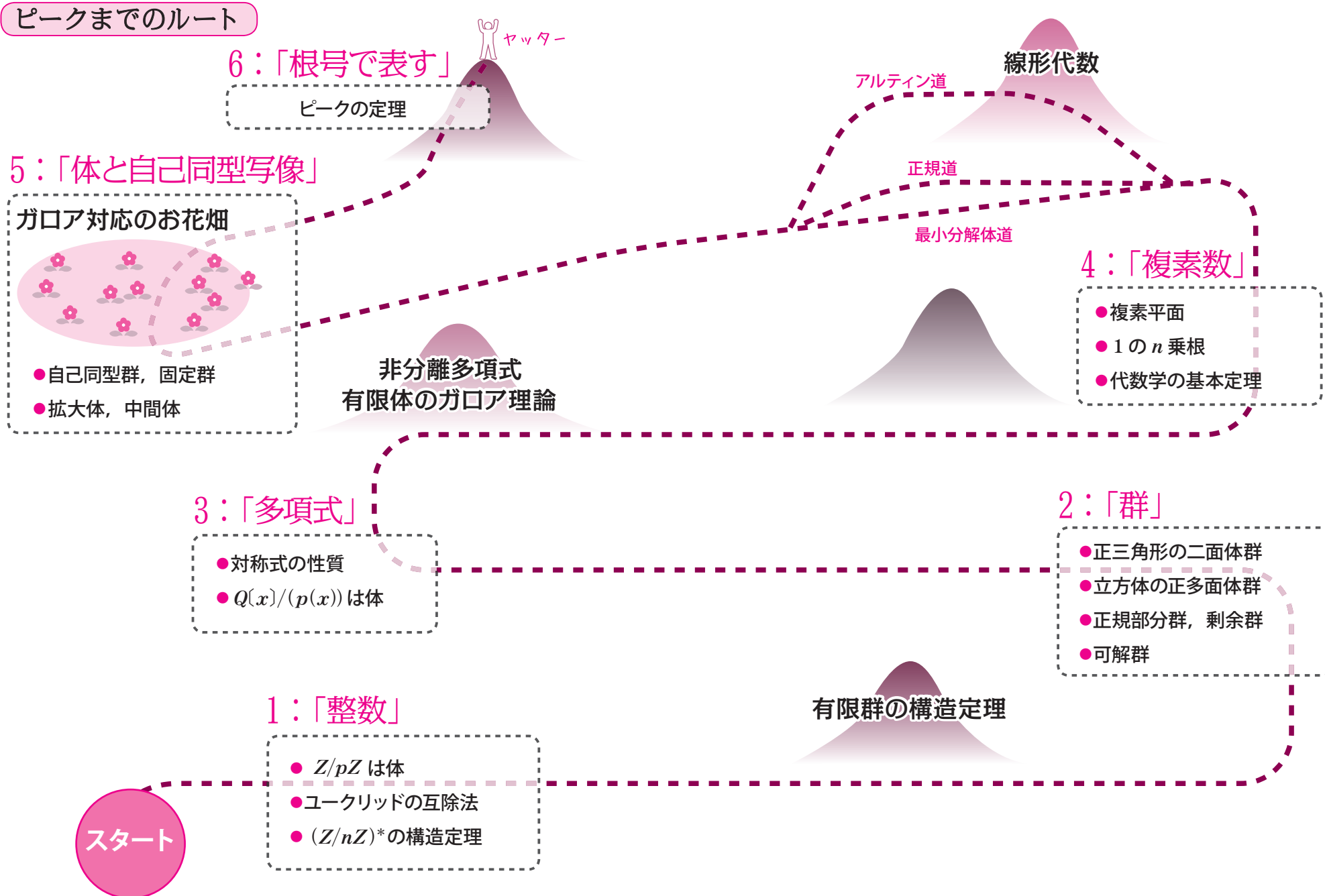
この本は、高校数学を履修した人に向けて、ガロア理論に手を触れてもらい組み立ててもらうことで、5次方程式が根号で解けない原理を理解してもらう本です。やさしく読めますが本格派なのです。

やさしく読めるための工夫の一つが、ルートの選択です。ピークの定理にたどり着くには、いくつかのルートがあります。この本では、これらの中からつねに一番やさしいと思われるルートを選びました。ピークの定理を証明するのに必要な定理がある場合でも、それが抽象的過ぎたり、証明が煩雑になる場合は、あえて避けることにしました。他の定理を組み合わせることで、これを代用しています。

縦走して特定の峰を目指すとき、尾根道をルートにとるといくつも山を乗り越えアップダウンを繰り返さなければならないものですが、巻き道（頂上を迂回する道）をとることでゆるやかに目的のピークに達することができます。この本では、読者の負担を減らすために巻き道をとっているところがいくつかあります。

次頁のイメージ図を眺めていただいてから、実際にどのようなルートをとってピークの定理まで到達するのか、ルートを解説しておきましょう。

ピークまでのルート



○ ルートの説明

登り口は、第1章「整数」です。ユークリッドの互除法、余りの計算から始まります。ここで早くも群の定義を紹介します。第2章の群のところでは定義をしようかとも考えたのですが、整数というとりつきやすい題材を通して群を実感してもらうのがよいだろうという判断から、ピークを目指すのに不可欠な「群」という装備を早めにお渡しすることにしました。

整数の章の最終目標は、既約剰余類群の構造の解明です。これはピークの定理の証明でも使われる事項で重要項目です。ピークの定理の証明のためには、有限生成アーベル群の基本定理を用意してもよいのですが、読みやすく証明を語るには線形代数の定理を積み重ねなければならないので避けました。巻き道をとったところです。

次に、第2章「群」へと進みます。正三角形の二面体群、立方体の正多面体群という具体的な群の例を通して、群についての重要な概念である剰余群、正規部分群を解説していきます。本書の特色の一つは、数学の概念を可視化していることですが、この章を読めば群を手にとるように実感することができるでしょう。しかも、この2つの例は3次方程式、4次方程式が根号で解けることの証明の伏線になっているのです。

群の章の後半は、あみだくじの群を扱います。数式（群の演算）を示すときは、図版での説明も入れましたから、演算を図上で確かめることができ読みやすくなっています。後半の目標定理は、「5本以上のあみだくじの群が可解群でない」という定理です。ここは、交換子群という概念を用意すると、数学的にはすっきりと証明することもできますが、なぜ4次以下と5以上に決定的な違いがあるのかが、具体的に分かるようにあみだくじを使って証明してみました。ここも巻き道をとったところです。

第3章は、「多項式」です。この章の初めでは、「対称式が基本対称式で

表せる」という定理とその証明のあらすじを紹介します。方程式の係数は、解の対称式になっていますから、この定理は方程式の理論を進めていく上で重要な定理です。第5章では当たり前のようにこの定理を使っていきます。

この章の後半は、整数における素数と多項式における既約多項式のアナロジーを推し進めて、整数で展開した理論を多項式にリフトアップしていきます。楽曲でいえば、整数で奏でられたメロディーが転調して多項式で出てくるような感じです。その展開の面白さににちょっとした感動を覚えるところでしょう。結論として得られる「既約多項式による体」は、第5章の基本的なフィールドとなります。

この第3章では、大きな選択をしました。それは方程式を考える多項式を有理数係数の多項式に限定したことです。専門書では、有理数係数の多項式以外も考え、平行して話を進めていくので、説明も煩雑になり、ただでさえ難しいガロア理論がより複雑になってしまうのです。専門書では、次頁の図の「非分離多項式」「有限体のガロア理論」という尾根を進むルートをとるのが普通です。本書ではこの小峰を巻いていきます。

第4章は、「複素数」です。この本では、読者に複素数の知識を仮定しませんが、複素数の定義から始めて解説していきます。この章の前半では、1の n 乗根を三角関数を作って書き下し、 $x^n - 1 = 0$ 、 $x^n - a = 0$ の解を複素平面上で実感してもらいます。この方程式の解が根号の意味するところですから、これが第6章で展開する理論の舞台となります。

この章の後半では、「すべての n 次代数方程式は複素数の中に解を持つ」という「代数学の基本定理」を証明します。これは第5章で体の拡大を考えると、そもそも方程式に解が存在するののかということを肯定的に解決してくれます。代数学の基本定理は、第5章の内容が空理空論に陥らないためにも重要な定理です。

第5章は、「体の拡大と自己同型群」がテーマです。拡大体の例をあげていく中で、自己同型群、ガロア拡大の概念を紹介していきます。

ここでは、方程式のガロア群の部分群と拡大体の中間体が1対1に対応するといういわゆる「ガロア対応」を説明します。

ここはガロア理論の華とでもいうべき箇所です。雲の上に一面のお花畑が広がっているような景色を見ることができます。啓蒙書のツアーでは、ここを向かいの山の中腹の山小屋から遠望するだけですが、この本のツアーの参加者には、このお花畑に実際に降り立ち高山植物の写真を撮ってもらいます。

このガロア拡大体の概念を定義するには大きく分けて3つのルートがあります。

ガロア拡大体の定義

- (1) 方程式の最小分解体
- (2) 有限次正規拡大体
- (3) (ガロア群の位数) = (拡大体の次数)

この本がとったルートは、(1) (最小分解体道) です。方程式の問題を扱うのですから、それから離れてしまう定義ではガロア拡大体を実感できないと思ったからです。ここも具体例で実感してもらおう本書のコンセプトにあったルート選択となっています。

(2) (正規道)、(3) (アルティン道) は方程式から離れてガロア拡大体を定義しています。

(3) は、アルティン流といわれる数学的にはすっきりとしていて魅力的な定義です。等式ですから、あとあとの証明の記述がずいぶんクリアになります。しかし、線形代数に慣れていないと扱えない上に自己同型群を抽象的なまま扱うのが難点です。

本書では、ガロア対応の実例を示した後で、ガロア対応の証明をします。啓蒙書ではなかなかフォローできていないところです。

第6章「根号で表す」では、いよいよピークの定理の証明に挑みます。章の冒頭では1の n 乗根が根号で表されることを具体的に計算で示します。1の n 乗根が根号で表されることは、ピークの定理から導かれる事実ですが、具体的な計算は他書ではなかなかお目にかかれないところです。

次に、3次方程式、4次方程式の解の対称性について調べます。第2章で手に入れた正三角形の二面体群、立方体の正多面体群という装備が大いに役立つところです。続いて、1の n 乗根が作る体、 $x^n - a = 0$ の解が作る体の構造を十分に調べます。根号で表される数とは、これらの方程式を繰り返して得られる数のことだからです。

後半では、第1章の最後の定理、第2章の群の理論、第5章のガロア対応の合わせ技で、最後の岩場を登ります。この岩場を登り切ったところにピークの定理があります。これで初等ガロア理論を制覇したことになります。第5章のお花畑に立った時の感動とはまた異なった感慨を持つことでしょう。ピークの定理登頂の余韻を楽しんでもらったところで、根号で解けない5次方程式を紹介します。

以上が、この本でとったピークの定理までのルートです。

さあ、準備はよろしいでしょうか。道のりは長いですが、ゆっくりでけっこうですので、一步一步、踏みしめながら、一緒に頂を目指しましょう。

1 最大公約数を求める

ユークリッドの互除法

最大公約数を求めるとき、中学生までは2数を素因数分解して、共通な素因数を探すという手順を踏んでいたと思います。2数の最大公約数を求めるには次のような方法もあります。

問 1.1 851, 185の最大公約数を求めよ。

理由はあとで説明することにして、次のように割り算を繰り返すと最大公約数が求まります。

$$\begin{array}{lcl} 851 \div 185 = 4 & \text{余り} & 111 \\ 185 \div 111 = 1 & \text{余り} & 74 \\ 111 \div 74 = 1 & \text{余り} & 37 \\ 74 \div 37 = 2 & \text{余り} & 0 \end{array}$$

これによって、最後の割り算で、割る数であった37が、851と185の最大公約数となります。

2数の最大公約数は、上の計算のように1つ前の式の「割る数」を「余り」で割る割り算を繰り返していくことで求めることができます。今まで2数を素因数分解し共通な素因数を探していた人からすれば、割り算を繰り返すだけで最大公約数が求められることは驚きではないでしょうか。

このような計算法は、**ユークリッドの互除法**と呼ばれています。

なぜこのような計算で最大公約数が求まるかを、初めにイメージで説明してみましょう。

851と185の最大公約数を求めることは、次のような問題を解くことと同じです。

正方形のタイルを用いて、たて185、よこ851の長方形を作ります。正方形の大きさをなるべく大きくとったとき、正方形の1辺の長さはいくらですか。

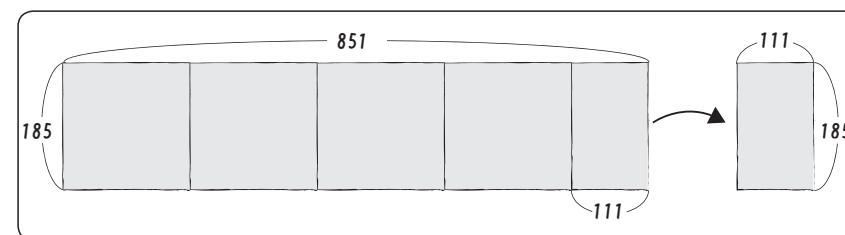
正方形のタイルを並べて長方形を作るのですから、長方形のたての長さ、よこの長さは、正方形の1辺の長さの倍数になっています。

逆にいうと、正方形の1辺の長さは長方形のたて、よこの長さの約数になっています。このうち、一番大きいものをとろうというのですから、答えは851と185の最大公約数になります。

851と185の最大公約数を g とし、1辺が g の長さの正方形のタイル（単位正方形と呼びましょう）で、たて185、よこ851の長方形を作ることができたします。

$$851 \div 185 = 4 \quad \text{余り} \quad 111$$

という割り算を、長方形に関する操作で表せば、次のようになります。



割り算は、たて185、よこ851の長方形から、1辺が185の正方形をとれるだけとることに対応します。たて185、よこ851の長方形も、1辺が185の正方形も、単位正方形できていましたから、こういう操作ができることに注意しましょう。

このように長方形から、短い辺の長さを1辺とした正方形をとれるだけとっていく操作を繰り返すと、いつかは長方形の余りなくピッタリと正方形がとれるときがきます。このとき、最後にとる正方形は単位正方形になります。

数学の言葉でもしっかりと説明しておきましょう。

定理1.1 互除法の原理

(x, y) で x と y の最大公約数を表すことにする。

a, b を自然数とする。 a を b で割った余りが r のとき、次が成り立つ。

$$(a, b) = (b, r)$$

a と b の最大公約数と、 a と b の割り算をしたときの割る数 b と余り r の最大公約数が等しくなるということです。

この定理を上にした具体的な計算に繰り返し用いると、

$$(851, 185) = (185, 111) = (111, 74) = (74, 37)$$

となります。851と185の最大公約数と74と37の最大公約数が等しくなるわけです。74は37の倍数ですから、74と37の最大公約数は、37と求めることができます。

割り算を繰り返し、最後に割り切れたときの割る数が最大公約数になっているのです。

割り算では、余りの数は割る数よりも小さくなりますから、余りは順次小さくなります。うまく割り切れず、最後には1になってしまう場合も考えられます。こういうときは、初めの2つの数の最大公約数が1です。 a と b の最大公約数が1のとき、 a と b は互いに素であるといいます。

証明 $(a, b) = g, (b, r) = h$ とおいて、実は $g = h$ であることを示しましょう。

a, b は g の倍数なので、自然数 a', b' を用いて、

$$a = a'g, b = b'g \quad \cdots \cdots ①$$

と書くことができます。

a を b で割った商を q とします。余りが r ですから、

$$a = qb + r \quad \cdots \cdots ② \quad \text{これより、} r = a - qb$$

これに①を代入して、 $r = a'g - qb'g = (a' - qb')g$

となり r も g を約数として持ちます。もともと b は g を約数として持ちますから、 g は b と r の公約数です。公約数は最大公約数以下ですから、 $g \leq h$ です。

また、 b, r は h の倍数なので、自然数 c', r' を用いて、

$$b = c'h, r = r'h$$

と書くことができます。②にこれを代入して、

$$a = qb + r = qc'h + r'h = (qc' + r')h$$

a は h を約数に持ちます。 b はもともと h を約数に持ちますから、 h は a と b の公約数です。公約数は最大公約数以下なので、 $g \geq h$ です。

$g \leq h$ かつ $g \geq h$ が示されたので、 $g = h$ です。 (証明終わり)

互除法は、次のような方程式の整数解を求めるときにも応用されます。

問1.2 次のそれぞれの式を満たす整数 x, y を1組求めよ。

$$(1) \quad 17x + 5y = 1$$

$$(2) \quad 15x + 6y = 9$$

$$(3) \quad 15x + 6y = 5$$

実際のところ、答えを見つけるだけなら x を1, 2, 3, ...と順に代入して、それに対する整数 y があるかを調べた方が早いのですが、先につながる話がありますので、ここは互除法を用いて解いてみましょう。

ポイントは、互除法を用いて左辺の式を係数の小さい1次式に変形していくところですね。このように $ax + by = d$ の形をした式の整数解を求める問題を1次不定方程式といいます。

17を5で割ると商が3、余りが2なので、 $17 = 5 \cdot 3 + 2$

$$17x + 5y = (5 \cdot 3 + 2)x + 5y = 5(3x + y) + 2x = 5z + 2x$$

5で括ると zとおく

ここで、 $z = 3x + y \cdots \cdots ①$ とおきました。