12 第１２回：互除法

きょうの予定

- 上限と最小公倍数.
- $\mathbf{Z}/p\mathbf{Z}$ の環の構造.
- ユークリッドの互除法・中国の剰余定理
- テストの予告
- 推薦図書

補講は行いません。

12.1 上限の概念

順序関係については §7.3.1 で述べたが、もう一度説明しておく。

12.1.1 順序関係

S2 項関係 $\preceq$ が、反射性・反対称性・推移性を持つとき、**順序関係**であるという。集合に一つの順序関係を与えたものを順序集合 (partially ordered set,poset) という。順序集合は $(X, \preceq)$ のように、集合 X と順序関係 $\preceq$ の組で表す。$x \preceq y$ のとき $\preceq$ **に関して** y **は** x **以上**であるという。

主な例は

- $(\mathbf{R}, \leq)$,
- $(\mathbf{N}, \preceq)$, ただし、$x \preceq y \overset{def}{\Longleftrightarrow} x|y$.
- $(\mathcal{P}(X), \subseteq)$.

２つの元 x, y が**比較不能である**とは、$x \preceq y$ でも $y \preceq x$ でも**ない**ことをいう。

順序集合 $(X, \preceq)$ と、部分集合 $Y \subseteq X$ から、部分順序集合 $(Y, \preceq_Y)$ が定義される, ただし、$y, z \in Y$ について

$$y \preceq_Y z \overset{def}{\Longleftrightarrow} y \preceq z.$$

12.1.2 最大・最小

$(X, \preceq)$ を順序集合とする。$M \in X$ が**最大元**であるとは、

$$\forall x \in X \, [\, x \preceq M \,].$$

最大元は存在するとは限らないがあれば唯一である。

同様に最小元が定義される。

$(\mathbf{N}, \preceq)$ には最大はないが、1 が最小となる。

12.1.3 上界と公倍数

a, b を順序集合 $(X, \preceq)$ の元とする。

a, b の両方以上の元をa, b **の上界**という. u が a, b の上界ならば、u 以上の元は皆 a, b の上界である。上界は存在するとは限らない。

（下界も同様に定義する。）

$(\mathbf{N}, \preceq)$ の場合は、a, b の上界を公倍数という。

12.1.4 上限と最小公倍数

a, b の上界の全体が最小元を持つとき、それを a, b の**上限**(最小上界,least upper bound, supremum) といい $a \vee b$, $\sup\{\, a, b \,\}$ などと書く。上限は存在しないときもあるが、自然な poset では存在することが多い。

$(\mathbf{N}, \preceq)$ の場合は、$a \vee b$ は最小公倍数にほかならない。従って存在する。

同様に a, b の**下界**, **下限** $a \wedge b$ が定義される。$(\mathbf{N}, \preceq)$ の場合は、a, b の下界は公約数、$a \wedge b$ は最大公約数にほかならない。

12.1.5 有限列の上限、下限

以上は 2 個の場合であるが、3 個以上 $a_1, a_2, \cdots, a_n$ についても上限が定義される。$a_1 \vee a_2 \vee \cdots \vee a_n$ または $\bigvee \{\, a_1, \cdots, a_n \,\}$ と書く。同様に下限も定義され、$a_1 \wedge a_2 \wedge \cdots \wedge a_n$ または $\bigwedge \{\, a_1, \cdots, a_n \,\}$ と書く。

これは、2 個の上限、下限があれば存在する、実際

$$(\cdots((a_1 \vee a_2) \vee a_3) \vee \cdots) \vee a_n$$

が上限となる。

12.1.6 任意個数の部分集合の上限

部分集合 $A \subseteq X$ についても $\bigvee A$ が定義される。ある元 $\boxed{c} \in X$ が A の上限であるための条件は、どの $x \in X$ についても

$$\forall a \in A\, [a \preceq x] \iff \boxed{c} \preceq x,$$

となることである。実際、「$\Longleftarrow$」を $x = c$ の場合に使えば c が A の上界であることがわかり、「$\Longrightarrow$」) より c が A の上界の中で最小であることがわかる。

実数の連続性の一つの表現は、

上界のある部分集合 $A \subseteq \mathbf{R}$ は上限を持つ

というものであった。

12.2 $\mathbf{Z}/p.\mathbf{Z}$ の代数的構造

$p > 1$ のとき、$\mathbf{Z}$ 上の同値関係 $x \equiv y \mod p$ の同値類集合を $\mathbf{Z}/p\mathbf{Z}$ と書いた。

命題 12.1 同値類集合 $\mathbf{Z}/p\mathbf{Z}$ には加算が

$$[x] + [y] := [x + y] \quad x, y \in \mathbf{Z}$$

により、乗算が

$$[x].[y] := [xy] \quad x, y \in \mathbf{Z}$$

により定義**できる**。

証明. この定義式が、代表元の取り方によらないこと、すなわち $a \equiv a' \mod p$ かつ $b \equiv b' \mod p$ ならば

$$a + b \equiv b + b' \mod p \qquad a.a' \equiv b.b' \mod p$$

を示せばよい。

そこで、$a \equiv a' \mod p$ かつ $b \equiv b' \mod p$ とする。定義より $a - a' = pn$, $b - b' = pm$ となる $n, m \in \mathbf{Z}$ がある。まず

$$(a + b) - (a' + b') = (a - a') + (b - b') = p(n - m)$$

より $a + b \equiv a' + b' \mod p$.

また

$$ab - a'b' = (a - a')b + a'(b - b') = pnb + a'pm = p(nb + a'm)$$

より $ab \equiv a'b' \mod p$.

以上により $a \equiv a' \mod p$ かつ $b \equiv b' \mod p$ ならば

$$a + b \equiv b + b' \mod p \qquad a.a' \equiv b.b' \mod p$$

が示され、定義が正当化された。 証終

$\mathbf{Z}/p.\mathbf{Z}$ は、$\mathbf{Z}$ の演算の持つ次の性質を遺伝する。

- 結合性 $(x+y)+z=x+(y+z)$, $(xy)z=x(yz)$,
- 可換性 $x+y=y+x$, $xy=yx$,
- 分配性 $x(y+z)=xy+xz$,
- 単位元 $0+x=x$, $1\,x=x$,
- x は和についての逆元 $-x$ を持つ： $x+(-x)=0$.

集合 M 上に 2 項演算 $x,y\mapsto x+y, x.y$ があり、$0,1$ を持ち、上の性質を満たすとき、$(M,+,0,.,,1)$ を可換環 (commutative ring) という。従って $(\mathbf{Z}/p.\mathbf{Z},+,[0],.,[1])$ は可換環である。

さらに、p が素数の場合には、

- $x\neq 0$ ならば積についての逆元 y がある：$xy=1$.

を満たし、$\mathbf{Z}/p.\mathbf{Z}$ は**体**(field) となる。これは次の節からわかる。

12.3 ユークリッド の互除法

12.3.1 最大公約数の求め方：ユークリッド の互除法

自然数 n,m の公約数 (caommon divisor) の全体を $CD[n,m]$ と書くことにすると、これは、最大公約数 $n\wedge m$ の約数の全体と一致する。

これは、次のようにして示される。$n<m$ としてもしてもよい。$n_0=m, n_1=n$ とおく。

n_0 を n_1 で割った余りを $n_2<n_1$, 商を q_1 とする：

$$n_0 \;=\; n_1q_1 \;+\; n_2. \tag{1}$$

この式より、明らかに $CD[n_0,n_1]=CD[n_1,n_2]$.

$n_2=0$ ならば、$CD[n_1,n_2]=M[n_1]$. 従って $n_1=n_1\wedge n_0$.

$n_2\neq 0$ とする。n_1 を n_2 で割った余りを $n_3<n_2$, 商を q_2 とする：

$$n_1 \;=\; n_2q_2 \;+\; n_3. \tag{2}$$

この式より、明らかに $CD[n_1,n_2]=CD[n_2,n_3]$. よって

$$CD[n,m]=CD[n_2,n_3].$$

$k\geq 3$ で $n_k\neq 0$ のとき同様に

$$n_{k-1} \;=\; n_kq_k \;+\; n_{k+1}. \tag{3}.$$

と続け、$n_{k+1} = 0$ となるとすると、

$$CD[n, m] = CD[n_1, n_2] = \cdots = CD[n_k, n_{k+1}] = \left\{ p \;\middle|\; p|n_k \right\}.$$

従って n_k が n, m の最大公約数となる。

以上がユークリッドの互除法である。アルゴリズムの原点と言われている。

12.3.2 ユークリッドの互除法の分析

ユークリッドの互除法のステップ (1) は次のように書ける。

$$\begin{pmatrix} n_0 \\ n_1 \end{pmatrix} = \begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} n_1 \\ n_2 \end{pmatrix}$$

また $k > 1$ のとき式 (k) は

$$\begin{pmatrix} n_{k-1} \\ n_k \end{pmatrix} = \begin{pmatrix} q_k & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} n_k \\ n_{k+1} \end{pmatrix}$$

となる。これより、もしも n_0, n_1 が互いに素ならば、次のような N がある。

$$\begin{pmatrix} n_0 \\ n_1 \end{pmatrix} = \begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} q_2 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} q_N & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

今

$$\begin{pmatrix} P_k & S_k \\ Q_k & T_k \end{pmatrix} := \begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} q_2 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} q_k & 1 \\ 1 & 0 \end{pmatrix}$$

とおくと、

$$P_1 = q_1 \qquad Q_1 = 1 \qquad S_1 = 1 \qquad T_1 = 0$$

と

$$\begin{pmatrix} P_k & S_k \\ Q_k & T_k \end{pmatrix} = \begin{pmatrix} P_{k-1} & S_{k-1} \\ Q_{k-1} & T_{k-1} \end{pmatrix} \cdot \begin{pmatrix} q_k & 1 \\ 1 & 0 \end{pmatrix}$$

より

$$S_k = P_{k-1} \qquad T_k = Q_{k-1} \qquad P_k = q_k P_{k-1} + S_{k-1} \qquad Q_k = q_k Q_{k-1} + T_{k-1}$$

となり、漸化式

$$x_k \;=\; q_k x_{k-1} + x_{k-2}$$

が $x = P, Q$ について成立していることがわかる。$\begin{pmatrix} q_k & 1 \\ 1 & 0 \end{pmatrix}$ の行列式は -1 だから、$\begin{pmatrix} P_k & P_{k-1} \\ Q_k & Q_{k-1} \end{pmatrix}$ の行列式は $(-1)^k$. 以上を用いると次のことがわかる。

12.3.3 互いに素な ℓ, m

ユークリッドの互除法を用いると、$(\ell, m) = 1$ のときに、$a\ell + bm = 1$ となる整数 $a, b \in \mathbf{Z}$ が存在することがわかる。

$\ell > m$ とし、ユークリッドの互除法に現れる商の列を $q_1, q_2, \cdots, q_N$ とする. このとき漸化式

$$\begin{aligned} x_2 &= q_2 x_1 + x_0 \\ x_3 &= q_3 x_2 + x_1 \\ x_4 &= q_4 x_3 + x_2 \\ x_k &= q_k x_{k-1} + x_{k-2} \qquad k \geq 4 \end{aligned}$$

を考え、これを 初期条件 $(x_0, x_1) = (1, q_1)$ で解いたものを $(P_1 = q_1, P_2, \cdots, P_N)$ とする。また、上の構成を $(q_2, q_3, \cdots, q_N)$ に対して行ったものの最初に 1 を加えたものを、$(Q_1 = 1, Q_2 = q_2, Q_3, \cdots, Q_N)$ とするとき、$P_N = \ell$,$Q_N = m$ となり、

$$P_N Q_{N-1} - Q_N P_{N-1} = \ell Q_{N-1} - m P_{N-1} = (-1)^N$$

となる。

例 $m = 82, \ell = 233$ のとき、商の列は $(2, 1, 5, 3, 4)$ となり、

k	1	2	3	4	5	6
q_k	2	1	5	3	4	
P_{k-1}	1	2	3	17	54	233
Q_{k-1}	0	1	1	6	19	82

たとえば $233 = 4 \times 54 + 17$, $82 = 4 \times 19 + 6$. PQ の中の隣接する 2×2 行列の行列式が $1, -1, 1, -1, \cdots$ であることに注意:

$$1 \cdot 1 - 2 \cdot 0 = 1, \qquad 2 \cdot 1 - 3 \cdot -1, \qquad 3 \cdot 6 - 17 \cdot 1 = 1.$$

$$19 \cdot 233 - 54 \cdot 82 = 4427 - 4428 = -1 = (-1)^5.$$

12.3.4 一次合同方程式

ℓ, m が互いに素であるとき、$[\ell]$ は環 $\mathbf{Z}/m\mathbf{Z}$ で可逆である。すなわち $[\ell][p] = [1]$ つまり

$$p\,\ell \equiv 1 \mod m$$

を満たす p がある。

証明 ユークリッドの互除法により

$$p\,\ell + q\,m = 1$$

となる p, q がある。従って

$$p\ell \equiv 1 \mod m,$$

すなわち環 $\mathbf{Z}/m.\mathbf{Z}$ で $[p]$ は $[\ell]$ の逆元となる。従って方程式

$$\ell x \equiv a \mod m$$

の解は

$$x \equiv pa \mod m$$

別の説明 ユークリッドの互除法により

$$p\ell + qm = 1$$

となる p, q がある。$x = pa$ とおくと

$$\ell x = \ell pa = a\ell p = a(1 - qm) \equiv a \mod m.$$

12.3.5 中国の剰余定理 (1)

ℓ, m が互いに素なとき、

$$x \equiv a \mod \ell, \qquad x \equiv b \mod m$$

は共通解 x を持つ。

解き方 前者の解は $x = a + \ell y (y \in \mathbf{Z})$ で与えられる。これが後者の解である条件は、

$$\ell y \equiv b - a \mod m$$

と書けるが、これは前節により解ける。$p\ell + qm = 1$ とすれば、$y = p(b - a)$ が解となる。従って $x = a + \ell p(b - a) = a(1 - \ell p) + b\ell p = mq.a + \ell p.b$ が解の一つとなる。これは直接にも確認できる。

例

$$19 \cdot 233 - 54 \cdot 82 = 4427 - 4428 = -1 = (-1)^5.$$

$$x \equiv a \mod 233, \quad x \equiv b \mod 82$$

を考える。

$$-19 \cdot 233 + 54 \cdot 82 = 1$$

より $x = 54 \cdot 82 \cdot a - 19 \cdot 64 \cdot b = -4428a + 4427b$ が解。

12.3.6 演習問題：中国の剰余定理 (2)

$n_1, n_2, \cdots, n_k$ のどの２つも互いに素であるとき連立合同式

$$x \equiv a_i \mod n_i \ (i = 1, 2, \cdots, k)$$

は解を持つ。

各 i について、n_i と $\ell_i := n_1 n_2 \cdots n_k / n_i$ とは互いに素なので、$p_i n_i + q_i \ell_i = 1$ となる p_i, q_i がある。このとき

$$q_i \ell_i \equiv \begin{cases} 1 & \mod n_i \\ 0 & \mod n_j \quad j \neq i \end{cases}$$

従って $x = q_1 \ell_1 a_1 + q_2 \ell_2 a_2 + \cdots + q_k \ell_k p_k$ が解を与える。

12.3.7 計算問題

[1] $6188 \wedge 4709$ を求めよ。
[2] $125a + 92b = 1$ となる a, b を求めよ。
[3] $256x \equiv 179 \mod 337$ を解け。
[4] $1215x \equiv 560 \mod 2755$ を解け。
[5] $x \equiv a \mod 13$, $x \equiv b \mod 17$ の一般解を求めよ。
[6] $x \equiv a \mod 25$, $x \equiv b \mod 27$, $x \equiv a \mod 59$ の一般解を求めよ。
[7] 次の連立合同式を解け。$x \equiv 3 \mod 8$, $x \equiv 11 \mod 20$, $x \equiv 1 \mod 15$.
[8] 次の連立合同式を解け。$x \equiv 1 \mod 3$, $x \equiv 4 \mod 5$, $x \equiv 2 \mod 7$, $x \equiv 9 \mod 11$, $x \equiv 3 \mod 13$.

12.4 参考図書

夏休みを利用して手応えのある本を読んでみよう。予備知識なしに読めて（やさしいということではないが）数学的内容が深い良書がたくさんある。本屋で探してみよう。

大学１年夏の段階の知識で読めるもので、目についた本を参考にあげておこう。

[1] 佐藤文広「これだけは知っておきたい　数学ビギナーズマニュアル」（日本評論社 1994）ISBN 4-535-78208-3.
数学のインフォーマルな面で重要な点を取り上げている。読み物風なので一度目を通してみよう。

[2] クヌース他（有澤誠他訳）「コンピュータの数学」（共立 1993）ISBN 4-320-02668-3.

TEX をつくったクヌースの講義録。原題は”Concrete Mathematics” で、現在の数学科の正規のカリキュラムでは余り取り上げないが数学的中身の濃い重要なテーマが扱われている。予備知識は要らない。

[3] 志賀浩二「数学が育っていく物語 方程式」(岩波 1994) ISBN4-00-007915-8.
高次代数方程式の解法、ガロア理論への入門。歴史的なエピソードも面白い。

[4] ヒンチン「数学の 3 つの真珠」(みすず書房 1979) .
初等的だが息の長い証明を理解しようとすることは有益である。

[5] ヴィノグラードフ (三瓶他訳)「整数論入門」(共立 1959)
合同式の解き方を詳しく述べている。演習問題は難しい。

[6] R. メーダー (井川俊彦監訳、時田進+宇田川誠一訳)『Mathematica プログラミング技法』(トッパン 1992)
マテマティカをプログラミング言語としても習得するには適した教科書。北大はキャンパスではマテマティカがどこでも使えるので、コンピュータ好きな人はマスターを試みよう。

[7] ニクリン・シャファレビッチ (根上生也訳)「幾何学と群」(シュプリンガー・フェアラーク東京 1993) ISBN 3-540-15281-4.
幾何学の原点を掘り下げる本。問題意識が数学の根底にあることを体験できる。「考える」ことが好きな人向き。

[8] 河野俊丈「組みひもの数理」(遊星社 1993) ISBN 4-7952-6874-6.
「組みひも」は現代数学の最前線の諸テーマに登場するが、予備知識なしに数学的な深さにすぐに近づくことのこtのできる数少ないテーマの一つである。

[9] 志賀浩二「数の大航海——対数の誕生と広がり」(日本評論社 1999) ISBN4-535-78289-X.
ネピアの死後初めて対数誕生の学問的ないきさつが明らかにしたもの。現代数学以前にも当然あった数学の深さを実感できる。

数学書 (和書) の紹介としてはインターネット上に次のようなものがある。

- http://www.math.sci.hokudai.ac.jp/~¡tosho/inhokudai/booklist.html
  北大数学の教官による紹介。5 年間更新されていない。
- http://math1.edu.mie-u.ac.jp/~kanie/book.htm
  網羅的だが、検索を使えばどういう本があるかがわかる。

なお、インターネット上での情報検索の入り口として私のところに次があるので利用してもらいたい。

- http://fcs.math.sci.hokudai.ac.jp/toc.html

数学科のホームページは

- http://www.math.sci.hokudai.ac.jp/index-j.html

12.5 テストの出題内容

講義で説明したことが身に付いているかど うかを確認する。

[1] 命題を論理式で表すこと、逆に論理式を言葉で表現すること.(cf. §2.5)

[2] 命題の否定を作ること。(cf.4.1–3,§5.4)

[3] $\forall\epsilon\exists\delta P \Rightarrow \forall\epsilon\exists\delta Q$ タイプの証明ができること。(§1.10,§4.4,§5.1,§6.3,§6.4)

[4] 集合演算の関係式を証明できること (§8.3)

[5] 全射・単射・全単射の定義、簡単な性質 (§8.4)

[6] 同値類集合上の演算 ($[x][y] = [xy]$ は well-defined であることを示せること。(§11.4, 命題 12.2)

[7] 上限の定義が述べられること。(§12.1)

[8] ユークリッドの互除法 §12.3 とその応用ができること。(§12.3.6)