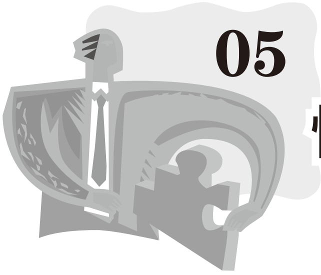

般

05 情報系の大学数学カリキュラム

鶴岡慶雅（東京大学） 田浦健次朗（東京大学）

大学での数学教育

コンピュータのための数学の基礎を本気で身に付けようとした場合，どのような数学をどのような順番で勉強したらよいのであろうか．大学で教えられている数学をすべて勉強(おさらい) するというのも１つの方法だが，大学数学の幅は広く，それらをすべてカバーしようとするのは忙しい社会人には難しい．

そこで本稿では，コンピュータに関する諸分野を学ぶ，いわゆる「情報系」の学生のための数学教育カリキュラムを参考に，情報処理に必要な数学を探ってみることにしよう．

図 -1 に，情報系のいくつかの学科の教育のカリキュラムから，数学に関する主なトピックを抽出したものを示す．各学科の学生が受講する数学に関する講義のシラバスを情報源として，教えられているトピックのまとまりに整理したものである．そのため，図中の項目名は科目名に対応しているわけではない．また，必修として学ぶべき内容は各学科によって異なっており，図中のすべての内容を情報系の学生が必修科目として学ぶわけではない．

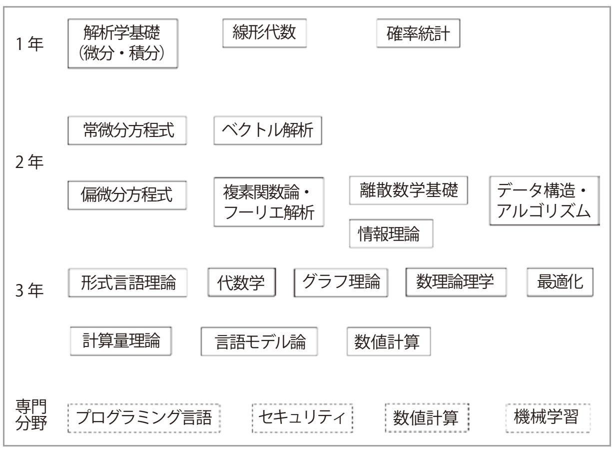

図 -1　情報系の数学カリキュラム例

以下，図中の各項目の内容を，情報処理，特に本特集で取り上げられている分野である，「プログラミング言語」，「数値計算」，「機械学習」，「セキュリティ（情報理論・符号理論）」との関連に触れつつ簡単に紹介する．

❖解析学（微分・積分）

関数の微分や積分について学ぶ大学数学の基礎である．多変数関数の「偏微分」を始め，以降の数学に必要な多くの基礎的な概念を学ぶ．加えて，ε–δ（イプシロン・デルタ）論法や ε–N 論法を用いて，実数の連続性や数列の極限などを厳密に議論するなど，大学数学らしい考え方が導入される．直感的な理解で事足りる高校数学と，抽象的かつ厳密な大学数学とのギャップに苦しむ学生も多い．そのためか，ε–δ 論法を含む厳密な数学的議論をあえて教えないこともある．

無限級数によって任意の関数を表現するテイラー展開，区分求積による多重積分，無限区間での積分などにも対応できる広義積分などの概念も導入される．特にテイラー展開は，数値計算や機械学習などの分野で関数を近似する手段として重要な役割を果たす．

❖線形代数

ベクトルや行列に関する計算やその性質に関する一般論を学ぶ．数値計算，機械学習，情報理論では，ベクトルや行列は最も基本的な表現形式の１つであり，線形代数はそれらの分野を学ぶ上では欠かすことのできない数学的な土台を提供する．

具体的には，行列の基本変形や，階数（ランク），行列式といった，行列に関する基本的な概念を学ぶ．また，ベクトル空間や，行列を抽象化したものとしての線形写像，ベクトル間の一次独立性，ベクトル空間の次元と基底といった概念も重要である．固有値と固有

ベクトルを利用した行列の対角化や，ベクトル空間の内積，2 次形式なども導入される．

❖確率統計

確率統計は，統計的機械学習や情報理論の理論的基盤であるだけでなく，観測・実験データを扱うあらゆる情報処理分野において重要な役割を果たす．

ランダム性や不確実性を持つ事象を表現する「確率変数」という考え方は，情報理論や統計的機械学習を支える最も基本的な概念の１つである．関連して，事象の独立性や条件付き確率，確率分布，期待値など，確率変数にかかわる諸概念を学ぶ．連続値をとる確率変数の確率分布を表すための確率密度関数も重要である．

データに関する仮説の有意性を検証するための「統計的検定」は，データを分析したり，実験結果を解釈する必要があるあらゆる研究分野で重要である．

ほかにも，ベイズ推定，母関数と特性関数，大数の法則，中心極限定理，確率過程などが，主要なトピックとなっている．

❖微分方程式

さまざまな微分方程式の解法と解の持つ性質を議論する．自然現象をモデル化する微分方程式としては，運動方程式がよく知られているが，ほかにも，熱方程式や電気回路の回路方程式など，さまざまな微分方程式が存在する．変数分離形の方程式や，定数係数の連立線形微分方程式などは解析的に解くことができるが，解析的に解くことが難しい場合は，有限要素法などの数値計算手法を用いる必要がある．

微分方程式論は，物理現象を扱う機械系や物理系，電気系の学生にとっては必須だが，純粋な情報系の学生の履修率は必ずしも高くないようである．

❖ベクトル解析

ベクトル解析では，微積分の発展として，多変数のベクトル値関数の扱いや幾何学的意味を学ぶ．具体的には，ベクトル場の曲線上の積分（線積分）や曲面上の積分（面積分），それらに関係する諸定理を学ぶ．ベクトル場の「発散」をある領域で積分したものと，その領域を囲む曲面でベクトル場を面積分したものが等しくなるという「ガウスの定理」はベクトル解析で学ぶ代表的な定理の１つである．ほかにも，グリーンの定理や，ストークスの定理などがある．

ベクトル解析も上記の微分方程式と同様，電磁界や流体，重力場など，物理的な自然現象を扱う分野では必須であるが，情報系の学科では必修ではないことが多いようである．

❖複素関数論・フーリエ解析

音声や画像などの信号を処理する場合，データの周波数領域での表現を利用することも多い．フーリエ変換は，時間領域のデータを周波数領域での表現に変換する数学的な操作である．実際の計算機での信号処理では，高速フーリエ変換アルゴリズムがよく使われる．

フーリエ解析とともに教えられることも多い「ラプラス変換」を利用すると，微分方程式を代数方程式として解くことができる．複素関数論は，フーリエ解析やラプラス変換のための数学的手段（留数定理を利用した複素積分など）を提供する．

❖離散数学基礎

要素の集まりとしての集合を数学的にきちんと定義し，それをもとに，べき集合，写像，関係，ブール代数などの概念を構築する．後述の代数学や数理論理学の基礎でもある．ある集合Ａの要素間の「関係」は，直積集合Ａ×Ａの部分集合としてフォーマルに定義される．任意の要素間に大小関係（のようなもの）が定義できる集合を半順序集合という．任意の要素の組に対して，最小上界と最大下界が存在するような半順序集合は「束」と呼ばれる．

❖代数学

我々が普段何気なく使っている「数」やそれらの間の「演算」を抽象化したものを考え，そこで成り立つ性質や構造を議論する．符号理論との関連が強いが，自然言語処理や音声認識に関する論文などで，動的計画法を一般化する手段として出てくることもある．

特定の演算の有無，各演算について閉じているか否か，結合法則が成り立つか否か，単位元があるか否か，などによって，「群」，「アーベル群」，「環」，「整域」，「体」などさまざまな代数系が存在する．有限個の元からなる体である「有限体」は，誤り訂正符号や疑似乱数の設計に用いられる．

❖情報理論

ある文字の情報の「量」をそれが起こる確率に基づいて定義し，平均情報量としての「エントロピー」を軸に，情報源や通信路の性質，符号化の性能などを議論する．データ通信はもちろん，圧縮，誤り訂正，暗号など，ビット列としてのデータを扱う多くの分野の理論的な基盤となっている．情報理論の概念が機械学習で使われることも多い．

情報理論や代数学をベースとして，データ圧縮や誤り訂正のための高性能な符号の具体的な構成法を考える符号理論や，公開鍵暗号など，セキュリティ分野において重要な役割をはたす暗号理論が発展している．

❖データ構造・アルゴリズム

プログラミングに関係するあらゆることの基本である．データ構造としては，コンピュータでデータを格納するための基本的なデータ構造である，配列，リスト，スタック，キュー，木などを学ぶ．

アルゴリズムとしては，データの効率的な検索を可能にする二分探索やハッシュ法，データ処理の基本であるソート（並び変え），大量のテキストから特定の文字列を効率的に検索するためのアルゴリズムなどがよく取り上げられる．計算完了までに，入力のサイズに対してどれだけのステップ（と記憶容量）を必要とするかはきわめて重要であり，各アルゴリズムの最悪計算量や平均計算量は，アルゴリズムを学ぶ上での中心的な要素となっている．

❖形式言語理論

有限オートマトンは，最も簡単な抽象化された計算機のモデルの１つであり，入力に応じて有限個の状態間を遷移する．文字列処理でよく用いられる「正規表現」で記述可能な正規言語（正則言語）は，有限オートマトンで受理することが可能である．再帰的な構文構造を持つ文脈自由言語を受理するためには，スタックを持つ有限オートマトン（プッシュダウン・オートマトン）を用いる必要がある．

チューリングマシンは，プッシュダウン・オートマトンよりも強力な抽象機械であり，通常のコンピュータで計算可能なすべての問題はチューリングマシンで計算することができる．その意味で，チューリングマシンは「万能」な計算機であり，計算可能性の問題を，チューリングマシンの停止性を通して考えることができる．

❖計算量理論

問題の本質的な「難しさ」を，それを解くために必要な計算や記憶領域の量に基づいて議論する．入力サイズに対して多項式時間で解ける問題クラス（クラスP）と，指数時間必要な問題クラスの区別が軸となる．有名なP≠NP予想とは，多項式時間で検証が可能な問題クラス（クラスNP）とクラスPが本質的に異なるという予想である．

ある問題の難しさを考える際には，論理変数の充足可能性問題（SAT）など，問題クラスが既知の問題からの多項式時間での還元可能性を通して議論することができる．重要な概念としては，NP完全（クラスNPに属する問題のうちで最も難しい），NP困難（クラスNPに属する問題よりも同等以上に難しい）などがある．たとえば，与えられた都市の集合を訪問する最短経路を探す「巡回セールスマン問題」は，NP困難な問題の１つである．

❖数理論理学

記号論理学とも呼ばれる．情報科学や計算機科学の基礎としての数理論理学は，機械による証明や計算の基礎となる数学である．構文的な推論規則から導かれる式（機械による証明に対応）と，構文に付与した数学的な「意味」のもとで真となる式とが，矛盾しないか否か（健全性）や，逆に後者が必ず推論規則から導かれるか否か（完全性）などが，いくつかの体系（命題論理や一階述語論理など）で議論される．

✣言語モデル論

（プログラミング）言語モデル論は，プログラムの正しさやプログラム言語の型システムや各種変換の正当性などを厳密に議論するための土台である．プログラム言語の仕様（プログラムの意味）の定義方法，プログラムの正しさを形式的に導出する体系（ホーア論理など）を学ぶ．またそれらの議論を，現実の言語の複雑さを捨象した単純な言語であるλ（ラムダ）計算を用いて行うのが典型で，そのもとで静的な型システムの型安全性（住井氏の記事参照）を証明する．

✣数値計算

数値解析とも呼ばれる．コンピュータで実数値を（近似的に）表現するための浮動小数点表現やそれによって生じる計算誤差（丸め誤差，桁落ち，情報落ち等）の話に始まり，連立一次方程式，行列の固有値問題，微分方程式などの数値解法を学ぶ．物体の運動のシミュレーションなどでよく使われるルンゲクッタ法は，微分方程式を数値的に解く代表的な手法の１つである．

台形則やモンテカルロ法を利用して積分を近似計算する方法や，最小二乗法による関数近似，高速フーリエ変換，乱数の発生手法（メルセンヌ・ツイスタ等）なども，数値計算のトピックスとしてしばしば取り上げられる．

✣最適化

数理計画と呼ばれることもある．与えられた基準に基づき，それを最大化（あるいは最小化）するような変数の値や組合せを効率的に求めるアルゴリズムを学ぶ．

最適化の問題は大きく，組合せ最適化（離散最適化）問題と連続最適化問題とに分けられる．「巡回セールスマン問題」や「ナップザック問題」は，組合せ最適化問題の例である．組合せ最適化のための手法として，動的計画法，整数計画法，分枝限定法などがある．

機械学習では，確率モデルのパラメータを尤度などの基準によって最適化するという状況が多く登場するが，これは典型的な連続最適化問題である．目的関数は多くの場合非線形となるが，勾配情報を利用した準ニュートン法などによって比較的効率的に最適解を求められることが多い．

目的関数と制約が線形の式で与えられる場合は，線形計画問題として定式化することができ，単体法（シンプレックス法）などの効率的な手法を用いることができる．線形計画問題よりも一般的な枠組みとして，凸最適化問題やそれに対する解法である内点法などがよく知られている．

✣グラフ理論

頂点（ノード）の集合とそれらを結ぶ枝（エッジ）の集合からなる「グラフ」の性質について学ぶ．コンピュータネットワークのように，物理構成が直接的にグラフと対応する分野はもちろん，機械学習における確率変数間の依存関係のような，概念レベルでグラフが構成されるような問題まで，幅広い応用が存在する．

有効グラフ，無向グラフ，平面グラフ，2 部グラフといったグラフの種類や，最短経路問題，最大流問題，最小全域木問題など，グラフ上で定義されるさまざまな問題とそれらを効率的に解くアルゴリズムを学ぶ．組合せ最適化とも強く関連している．

情報処理と数学

以上，情報処理と関係の深い数学を駆け足で紹介してきたが，本文中でも言及しているように，コンピュータに関するすべての分野に，これらの数学が全部必要とされるわけではない．情報処理のある特定の分野に必要な数学というように限定すれば，図 -1 に示した項目の中で 4 つか 5 つ程度というのが平均的ではなかろうか．数学の効率的な学びなおしのきっかけという意味で，本稿が少しでも役立てば幸いである．

(2015 年 3 月 11 日受付)

鶴岡慶雅（正会員）■ tsuruoka@logos.t.u-tokyo.ac.jp
2002 年東京大学大学院博士課程修了．博士（工学）．マンチェスター大学研究員などを経て，2009 年北陸先端科学技術大学院大学准教授．2011 年より東京大学大学院工学系研究科准教授．自然言語処理，ゲーム AI 等に関する研究に従事．

田浦健次朗（正会員）■ tau@eidos.ic.i.u-tokyo.ac.jp
1997 年理学博士（論文）取得．1996 年より，東京大学大学院理学系研究科情報科学専攻助手などを経て，2002 年より，東京大学大学院情報理工学研究科准教授．並列・分散処理，プログラミング言語などに関する研究に従事．