数学の勉強の仕方について

黒木 玄*

最終更新: 2002 年 6 月 18 日午前 10 時半頃†

目 次

*kuroki@math.tohoku.ac.jp

†この文書は東北大学大学院理学研究科数学専攻の大学院クラス・セミナーの受講者に配布するために 2002 年 6 月 5 日に作成され, 2002 年 6 月 11 日に配布された. その後の誤植の訂正に関しては院生の千田雅隆氏のお世話になった.

1 論理的に厳密に理解すること

1.1 何が仮定で何が結論なのかを正確に理解しているか?

さすがに仮定と結論が何であるかさえ理解してなければお話にならない.

どうしてそのように仮定するか, どうして結論をそのような形で述べるかについても考えた方が良い. 仮定 (もしくは結論) が成立している例と成立してない例にはどのようなものがあるかについても考えよう.

セミナーのときには仮定と結論を先に述べて, そのあいだを埋める議論は後で説明した方が良い. 仮定を述べて, 議論や証明を説明して, 最後に結論を説明するのは好ましくない. 結論はできるだけ早く述べるようにする.

1.2 登場するすべての数学用語の定義を理解しているか?

理解してない用語が一つでもあれば標準的な教科書などで調べる. 抽象的で意味がわからない定義の場合はどのような例があるかを調べる.

1.3 すべての文の証明の詳細を完璧に理解しているか?

単に「……である」と書かれていても, それに証明を付けようとすると結構面倒でかなり長くなる場合がある. しかし, たいていの場合は, 単純な論理的推論だったり, よく使われる議論の適用例になっている. 単純なことは単純であることが納得できるまで時間をかけて理解するようにつとめ, よく使われる議論の適用例であればそれが実際によく使われる議論であることが納得できるまで色々調べてみなければいけない.

1.4 説明のギャップの埋め方を理解しているか?

読者は説明のギャップを埋めて論理的なギャップが生じてないことを確かめる必要がある. たとえば, “It is easy to see that ...” (……であることが容易にわかる), “We may assume that ...” (……であると仮定してよい), “It is enough to show that ...” (……であることを示せば十分である) のように説明されている部分に論理的なギャップが生じない理由を理解しているか? あらゆることを詳細に説明するのは不可能だし, 可能だとしても能率が悪いので, 数学の文献には必ずこのような文章があらわれることになる.

1.5 証明抜きで使われる「大定理」の内容を正確に理解しているか?

可能な限り「大定理」の周辺の事柄について調べておいた方が間違いが少なくなる. 証明や応用や例についても調べておいた方が良い.

1.6 例を挙げよという質問に答えられるか?

自分自身がどれだけ理解しているかをチェックするためには, 例についてどれだけ知っているかを自問してみれば良い. セミナーの時間にも「例にはどのようなものがあるか?」

と質問されることになるだろう[1].

2　数学の教養

2.1　教養を身に付けるためには膨大な時間が必要

数学科の大学院に入学して難しそうに見える数学の本をセミナーで読み出すと,「論理的に理解できないだけではなく, そもそも何をやっているかがわからないので, 全然理解した気分になれない」と感じる人がたくさん出て来る.

その最大の原因は数学の教養が足りないことである. 数学に限らずあらゆる分野において教養を身に付けるためには膨大な時間が必要になる. しかも凡人が専門的な教養を身に付けるためには「寝ても覚めてもそれについて考え続ける」ほど熱中する時期が必要だと思う.

いずれにせよ, 専門的な数学を理解するためには広さと深さの両面において十分な数学的教養が不可欠である. 教養抜きでは大学院のセミナーで読んでいる数学の本の内容は何も理解できないだろう. だから, 教養が身に付かない限り, 大学院の厳しいセミナーに耐え続けても何も残らない可能性が高い[2].

2.2　数学的教養とは何か?

数学の教養とは数学に関わるあらゆる事柄のことである.

まず, 現代数学に関する基礎的な知識. 学部レベルの教科書に書いてある代数学, 解析学, 幾何学に関する基礎的な知識は当然数学の教養である. 単に抽象的な定義や定理について知っているだけではなく, 基本的な具体例について知っていることも重要である.

次に, 数学をやるときの基本的な態度. 論理的に正確に理解すること, 具体例をいじってみること, 数学の質問の仕方, 友人と数学について話すこと, 数学のノートの書き方, 計算用紙の使い方, などなど基本的な素養とみなせることはたくさんある.

さらに, 数学に関わる雑多な知識. 数学のあらゆる側面を数学科で教えているわけではない. たとえば, 物理で数学がどのように使われているかは物理を学ばなければ理解できないし, 様々な数学的概念の由来を知るためには数学の歴史にも興味を持つ必要がある.

数学に関わるあらゆることに熱意を持ってどれだけ時間をかけたかでその人の数学的教養の広さと深さが決まるのである.

2.3　基本的な知識の身に付け方

「数学に関わるあらゆることを全部やれ」と言われても困るだろうし, 現実問題不可能だと思うので, ここでは可能でかつすぐに役に立ちそうなことを紹介しよう.

たとえば, Euler の函数 $\varphi(n)$ (n は正の整数) が今読んでいる本に登場したとしよう. (ここでは, $\varphi(n)$ は $1 \leq m \leq n$, $(m,n) = 1$ となる整数 m の個数であると定義されているとする.) もしくは, 巡回群の生成元を選ぶ話が登場したとしよう.

---

[1]「どのような面白い例があるか?」という質問は内容を理解してない場合でも可能でしかも有益である.

[2]これは数学の大学院に限らない. 大学院においては, 皆が「十分な教養を身に付けて専門的な事柄を正確に理解すること」を最低限の目標とし,「まだ誰も理解してないことを自分自身の力で研究する」ところまでたどり着くことが望ましい.

すでに数学の基礎的知識を身に付けている人であれば,「$\varphi(n)$ は位数 n の巡回群の生成元の取り方の個数に等しいこと」や「$\varphi(n)$ は乗法群 $(\mathbb{Z}/n\mathbb{Z})^\times$ の位数に等しいこと」について知っているだけではなく, 巡回群や有理整数環の剰余環や有限生成 Abel 群一般の構造に関する基本的な事柄についても知っているはずである. そして,「Euler の函数は乗法的な数論的函数[3]の典型例であること」や「素数の巾 p^e に対して $\varphi(p^e) = p^{e-1}(p-1)$ が成立すること」についても当然知っているだろう.

もしもこの程度のことさえ知らないとすれば, Euler の函数や巡回群が登場する部分の議論を滑らかに理解することはできず, ものすごくギクシャクしてしまうことになる.

基本的な知識が足りないせいでギクシャクしてしまうのはそれがその人の実力なのだから仕方がない. 問題なのはギクシャクしてしまった同じ項目についてギクシャクすることを何度も何度も繰り返してしまうことである. 一度ギクシャクしてしまったならば関連の項目の周辺をよく勉強しておかなければいけない.

問題はその勉強の仕方である. 単に教科書を引いて調べるだけではいけない. 過去にやった勉強よりも深く理解するようにしなければいけない. 過去のやり方が駄目だったから基本的なことを理解できてないのだ. 同じことを繰り返すだけではきっと駄目だろう.

特に注意しなければいけないことは, **より一般的な理論**と**特殊な具体例**の両方を押さえておくように努力することである.

2.4 より一般的な理論を押さえておくこと

まず,「より一般的な理論を押さえておくこと」を具体的な例によって説明しよう.

Euler 函数について, 正の整数 n が $n = p_1^{e_1} \cdots p_r^{e_r}$ と素因数分解されているとき $\varphi(n) = \varphi(p_1^{e_1}) \cdots \varphi(p_r^{e_r})$ が成立することは同型 $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{e_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r^{e_r}\mathbb{Z}$ から容易に導かれる[4]. この同型は中国式剰余定理の簡単な応用例である[5]. この意味で中国式剰余定理は Euler 函数の乗法性の一般化とみなせる.

巡回群は 1 つの元から生成される Abel 群である. 位数 n の有限巡回群は $\mathbb{Z}/n\mathbb{Z}$ に同型であり, $\mathbb{Z}/n\mathbb{Z}$ の構造論は中国式剰余定理の最も簡単な応用先である. 巡回群の構造論の有限生成 Abel 群への拡張が有限生成 Abel 群の基本定理である. さらに, 有限生成 Abel 群の基本定理は単項イデアル整域上の有限生成加群の構造論すなわち単因子論に拡張される[6]. そして, 体 k (たとえば $\mathbb{C}$) 上の 1 変数多項式環 $k[x]$ 上の有限生成加群の構造論から, 行列の Jordan 標準形の理論を導くことができる[7]. 体は自明に単項イデアル整域であ

---

[3]正の整数に対して定義された複素数値函数を数論的函数と呼ぶ. 数論的函数 $f(n)$ が乗法的であるとは $(m,n) = 1$ ならば $f(mn) = f(m)f(n)$ が成立することである. f が乗法的な数論的函数であり, 正の整数 n が $n = p_1^{e_1} \cdots p_\nu^{e_\nu}$ と素因数分解されているとき, $f(n) = f(p_1^{e_1}) \cdots f(p_\nu^{e_\nu})$ が成立する.

[4]$\varphi(n)$ が $(\mathbb{Z}/n\mathbb{Z})^\times$ の元の個数に等しいことと, $(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{e_1}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_r^{e_r}\mathbb{Z})^\times$ より導かれる.

[5]$\mathbb{Z}$ に関する基本的な事実しか使わない証明は次の通り. 環準同型 $f : \mathbb{Z} \to \prod_{i=1}^r \mathbb{Z}/p_i^{e_i}\mathbb{Z}$ を $f(x) = (x \bmod p_i^{e_i})_{i=1}^r$ と定める. f の核が $n\mathbb{Z}$ であることがすぐにわかるので, f が全射であることを示せばよい. $n_i = n/p_i^{e_i}$ と置くと, $n_1, \ldots, n_r$ の最大公約数は 1 なので, Euclid の互除法より, ある整数 $m_1, \ldots, m_r$ が存在して $a_1n_1 + \cdots + a_rn_r = 1$ が成立する. このとき, $a_in_i \equiv \delta_{i,j} \pmod{p_j^{e_j}}$ であるから, 任意の $m_1, \ldots, m_r \in \mathbb{Z}$ に対して, $f(m_1a_1n_1 + \cdots + m_ra_rn_r) = (m_i \bmod p_i^{e_i})_{i=1}^r$. これで f が全射であることがわかった.

[6]$\mathbb{Z}$ は単項イデアル整域の最も基本的な例であり, 有限生成 Abel 群は $\mathbb{Z}$ 上の有限生成加群に等しい. 体上の 1 変数多項式環も単項イデアル整域の基本的な例である. $\mathbb{Z}$ のような数の世界と多項式のような函数の世界は似ている.

[7]たとえば, 堀田良之著『代数入門——群と加群——』(数学シリーズ, 裳華房) [5], 堀田良之著『加群十話——代数学入門——』(すうがくぶっくす 3, 朝倉書店) [6], 森田康夫著『代数概論』(数学選書 9, 裳華房) [7] では実際そのようなやり方で Jordan 標準形を導いている. 佐武一郎著『線型代数学』(数学選書 1, 裳華房) [2] は巾零行列の構造論から Jordan 標準形を導いている. どちらの方法も面白いので学んでおく価値が

る. 通常体上の加群はベクトル空間と呼ばれる. 体上の有限生成加群と有限次元ベクトル空間は同じものである. 有限次元ベクトル空間の理論は単純だが応用範囲が極めて広く, 大学における教養科目の一つになっている. 体の次に簡単な可換環である単項イデアル整域上の有限生成加群の理論は有限次元ベクトル空間の理論よりも少し複雑だがそんなに難しくはなく, 特殊な場合および重要な応用先として有限生成 Abel 群の基本定理や Jordan 標準形の理論を含んでいる.

それでは単項イデアル整域の次に扱い易い可換環は何だろうか? この問いに対する回答は立場によって様々だと思われるが, 一つの回答は Dedekind 整域である. Dedekind 整域の典型例は代数体の整数環であり, 数論における最も基本的な研究対象である[8].

2.5 特殊な具体例を押さえておくこと

次に「特殊な具体例を押さえておくこと」の一例を示そう.

自然に現われる位数 n の巡回群の実例に $\mathbb{C}$ の中の 1 の n 乗根全体のなす群がある. その生成元の全体は $\{\,\zeta_n^i \mid 1 \leq i \leq n,\ (i,n)=1\,\}$ ($\zeta_n = \exp(2\pi\sqrt{-1}/n)$) に一致し, その元の個数は $\varphi(n)$ に等しい.

$\mathbb{Q}(\zeta_n)/\mathbb{Q}$ の Galois 群の元の $\mathbb{Q}(\zeta_n)$ への作用は 1 の n 乗根全体のなす位数 n の巡回群の自己同型を誘導し, それによって $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ の Galois 群と位数 n の巡回群の自己同型群のあいだの同型が定まる[9].

標数 p の有限体 $\mathbb{F}_{p^e}$ の乗法群 $\mathbb{F}_{p^e}^\times$ は位数 p^e-1 の巡回群をなす. これも自然に現われる巡回群の実例である. p^e-1 は p で割り切れない. 逆に, n が p で割り切れない正の整数ならば, ある正の整数 e が存在して $\mathbb{F}_{p^e}^\times$ は位数 n の巡回部分群を含む[10].

たとえば, $\mathbb{F}_{64}^\times$ は位数 $63 = 3^2\cdot 7$ の巡回群をなすので, 位数 3, 3^2, 7 の巡回部分群を含む. $\varphi(11)=10$ なので $\mathbb{F}_{2^{10}}^\times = \mathbb{F}_{1024}^\times$ は位数 11 の巡回群を含む. 実は $\mathbb{F}_{1024}$ は乗法群が位数 11 の巡回群を含む標数で 2 であるような最小位数の有限体である. 実際, $2^1-1=1$, $2^2-1=3$, $2^3-1=7$, $2^4-1=15=3\cdot 5$, $2^5-1=31$, $2^6-1=63=3^2\cdot 7$, $2^7-1=127$, $2^8-1=255=3\times 5\times 17$, $2^9-1=511=7\cdot 73$, $2^{10}-1=1023=3\cdot 11\cdot 31$. このように数値的な実例で感じをつかんでおくことも大事なことだと思う.

『岩波数学辞典第 3 版』 [4] において Euler 函数 $\varphi(n)$ の説明は「189 数論的関数」の項目 C にある (488 頁). そこには Euler 函数の他に Möbius 函数 $\mu(n)$ に関する説明も書いてある. 正の整数 n に対して $\mu(n)$ は, $\mu(1)=1$, n が相異なる r 個の素数の積のとき $\mu(n)=1$, それ以外のとき, すなわち n がある素数の 2 乗で割り切れるとき $\mu(n)=0$ と定義される. このとき, Euler-Riemann のゼータ函数を $\zeta(s)$ と書くと,

$$\frac{1}{\zeta(s)} = \prod_{p:\text{prime}} (1-p^{-s}) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} \qquad (\operatorname{Re} s > 1).$$

せっかく Möbius 函数の存在を知ったなら, この公式まではたどり着きたい.

ある.

[8] 体 k 上の affine smooth curve の affine coordinate ring も Dedekind 整域になる. たとえば, $\mathbb{C}$ 上の楕円曲線 $y^2 = x^3 - x$ 上の affine coordinate ring $\mathbb{C}[x, \sqrt{x^3-x}] = \mathbb{C}[x,y]/(y^2-x^3+x)$ は Dedekind 整域である. 整数の世界と曲線上の函数の世界は非常に似ている.

[9] たとえば, 森田『代数概論』 [7] の定理 6.4 を見よ.

[10] 証明は次の通り. ある正の整数 e が存在して p^e-1 が n で割り切れることを示せば良い. n は p で割り切れないという仮定から, $p \bmod n \in (\mathbb{Z}/n\mathbb{Z})^\times$ である. よって, $p^{\varphi(n)} \equiv 1 \pmod n$. すなわち, $e=\varphi(n)$ と置けば p^e-1 は n で割り切れる.

なお, 岩波数学辞典第 3 版では Möbius の反転公式を系由して

$$\sum_{d|n} \varphi(d) = n$$

を得ているが, 位数 n の巡回群の生成元の取り方の個数が $\varphi(n)$ に等しいことを利用して, 直接に証明することもできる[11].

特殊な数だけではなく, 特殊な函数についても色々感じをつかんでおくことは大事なことである. 他にも, 特殊な方程式, 特殊な写像, 特殊な群, 特殊な環, 特殊な加群, 特殊な体, 特殊な多様体, などなどについて, 機会があるごとに感じをつかむために色々いじってみるべきである.

3 数学の世界の散歩・散策のすすめ

数学を理解することは与えられたことをこなすだけでは不可能である.

そのことは小学校から高校にかけて, 算数や数学が得意な人とそうでない人が算数や数学とどのように向き合っていたかを思い出せば明らかだと思う. 算数や数学が得意な子供は他人に言われなくても色々勝手にやってしまうから得意になるのだ. 過去に算数や数学が得意であっても色々勝手にやってしまうことを忘れると数学があっというまに苦手になってしまう.

子供のときには勝手にやるべき題材の多くを大人が用意してくれた. しかし, 大学生以上は大人とみなされ, 大人は大人に勝手にやるべき題材を用意してくれない. 各人が自分の意志で勝手にやるべき題材を見付けなければいけない. それをやらないとあっというまに数学が苦手になってしまうだろう[12].

数学科の大学院生は学部時代に習ったこと (もしくは習ったことになっているはずのこと) について勝手に色々勉強し直さなければいけない.

おすすめなのは, 過去に習ったことの周辺を散歩・散策してみるつもりで勉強し直すことである. 散歩・散策なのだから, あせらず風景を眺めながら進むことが重要である.

たとえば, 学部の代数学の講義や演習で群や環や加群や体などなどについて習ったはずである. それらについて勉強し直すときには, 具体的にどのような群や環や加群や体が登場し, それらの全体がどのような風景をなしているかをよく眺めてみるべきである[13].

3.1 群にはどのようなものがあるだろうか?

1 つの元から生成される巡回群は群の中で最も簡単な群のはずである. 巡回群の全体はどのような風景をなしているか? 巡回群だけでもよく眺めてみれば色々楽しめるはずである.

[11]実際, 次のようにして証明される. G は位数 n の巡回群であるとする. $x \in G$ に対して x から生成される G の巡回部分群の位数を $\operatorname{ord} x$ と書くことにする. $\operatorname{ord} x$ は n の約数になる. そこで, n の約数 d に対して, $\operatorname{ord} x = d$ をみたす $x \in G$ の全体の集合を A_d と書くことにする. G は A_d たちの disjoint union になる. G に含まれる位数 d の巡回部分群は唯一なので, A_d の元の個数は $\varphi(d)$ であることがわかる. よって, $\sum_{d|n} \varphi(d) = n$ である.

[12]これは数学に限らず, あらゆる分野でそうだと思う.

[13]I. R. シャファレヴィッチ著『代数学とは何か』(シュプリンガー・フェアラーク東京) [3] は代数学の世界の散策のために非常に便利な面白い本である. この本の素晴しいところは純代数にこだわることなく, 解析学や幾何学からも自由に題材を選んでいることである. やはり数学は一つであり, 「代数学とは何か」を理解するためには数学全体に関する素養が必要なのである.

巡回群の次に簡単な群は何だろうか? 巡回群とは 1 つの元から生成される Abel 群のことである. よって, 有限個の元から生成される Abel 群すなわち有限生成 Abel 群は巡回群の次に調べる群の有力候補であると考えられる. 実際, 代数学の教科書や講義の中には有限生成 Abel 群の基本定理の解説があるはずである. それによって, 有限生成 Abel 群の構造もよくわかる.

それでは, 非 Abel 群すなわち非可換群にはどういう例があるのか? $n > 2$ 次の置換群 S_n は非可換であり, $n > 3$ ならば交代群 A_n も非可換である. $n \geq 5$ であれば A_n は単純群になるのであった. S_n の生成元として $s_i = (i, i+1)$ $(i = 1, \dots, n-1)$ が取れて, s_i は次の基本関係式を満たしている:

$$\begin{aligned} &s_i^2 = 1 \qquad (i = 1, \dots, n-1), \\ &s_i s_j s_i = s_j s_i s_j \qquad (|i-j| = 1), \\ &s_i s_j = s_j s_i \qquad (|i-j| > 1). \end{aligned}$$

これは「あみだくじ」の関係式になっている[14]. 置換群は行列式の定義などにも登場するのであった.

実数や複素数で構成された群には加法群 $\mathbb{R}$ や乗法群 $\mathbb{C}^\times$ や, $SU(n)$ や $SL_n(\mathbb{C})$ のような行列 Lie 群がある. n 次元 Euclid 空間の自己同型群 (Euclid 群と呼ぶ) のような例もある. $SU(2)$ は位相的には 3 次元球面 S^3 と同相である.

上半平面 $\mathfrak{H} = \{\, \tau \in \mathbb{C} \mid \operatorname{Im} \tau > 0 \,\}$ には一次分数変換によって, $SL_2(\mathbb{R})$ が作用しているので, $SL_2(\mathbb{R})$ の離散部分群 $SL_2(\mathbb{Z})$ も作用している. この設定は数論において基本的でかつ極めて重要である.

置換群 S_n は有限集合 $\{1, 2, \dots, n\}$ からそれ自身への集合としての同型 (すなわち全単射) 全体のなす群である. 一般に数学的な対象 X を与えればそれからそれ自身への適切な意味での同型写像全体は群をなす. その群は X の対称性であると解釈できる.

体の Galois 拡大 L/K に対して, K の元を固定する L からそれ自身への体の同型写像全体は Galois 群 $\mathrm{Gal}(L/K)$ をなす. 少年 Galois は方程式の解の置換のなす群として Galois 群の概念を発見したのであった. そのとき, 方程式の性質を方程式の対称性を調べることによって研究するという素晴らしいアイデアが誕生したのである.

可微分多様体 M からそれ自身への微分同相写像全体は群をなす. これは置換群の可微分多様体版であるとみなせる.

$\mathbb{R}^n$ からそれ自身への線型同型写像全体は一般線型群 $GL_n(\mathbb{R})$ をなす. 自然な内積が入っている $\mathbb{R}^n$ からそれ自身への内積を保つ線型同型写像全体は直交群 $O(n)$ をなす. $O(n)$ は $\mathbb{R}^n$ の鏡映変換と回転から生成される群である.

群の概念は対称性の概念の抽象化である. だから, 抽象的な群が与えられたとき, その群はどのような数学的対象の対称性になっているか, というのは基本的な問題になる. 逆に与えられた数学的対象が何らかの綺麗な性質を持っているとき, その裏に隠された対称性を明らかにし, 群の表現論の立場からの理解を目指すことも重要な問題である.

3.2 可換環とそれ上の加群にはどのようなものがあるだろうか?

まず, 有理整数環 $\mathbb{Z}$ は小学生のときからお世話になっている最も身近な可換環であろう. $\mathbb{Z}$ 上の有限生成加群と有限生成 Abel 群は同じものである.

[14] 置換群の基本関係式から $s_i^2 = 1$ を取り除いたものは組紐群 B_n の関係式に等しい. $s_i s_j s_i = s_j s_i s_j$ は組紐関係式と呼ばれたり, Yang-Baxter 方程式と呼ばれることがある.

有理数体 $\mathbb{Q}$ やその完備化である実数体 $\mathbb{R}$ やそれに $\sqrt{-1}$ を添加して得られる複素数体 $\mathbb{C}$ も可換環である. $\mathbb{R}$ (もしくは $\mathbb{C}$) 上の有限生成加群は有限次元実ベクトル空間 (もしくは有限次元複素ベクトル空間) と同じものである. それらに関する理論は大学における教養科目の一つになっている.

体 k 上の 1 変数多項式環 $k[x]$ は中学生のときに 1 変数の文字式について習うのでこれもまた身近な可換環である. しかし, $k[x]$ 上の有限生成加群の概念は大学の数学科で扱う対象になってしまう. $k[x]$ 上の有限生成加群の理論から Jordan 標準形の理論を導くことができる.

有理整数環 $\mathbb{Z}$ 上もしくは体 k 上の n 変数多項式環は複数の文字からなる式の世界であり, n 変数多項式環上の有限生成加群の世界は非常に複雑になる. 任意の有限生成環は $\mathbb{Z}$ 上の n 変数多項式環の剰余環になっている. 体 k 上有限生成な環は k 上の n 変数多項式環の剰余環になっている. この意味で n 変数多項式環は基本的な環である.

ここで, 体 k 上有限生成な環の理論は多変数連立代数方程式の理論の抽象化であるとみなせることを説明しよう.

R は体 k 上 $\xi_1, \dots, \xi_m$ で生成される可換環であるとする. 多項式環 $k[x_1, \dots, x_m]$ から R への k 上の環準同型で x_i を ξ_i に対応させるものが唯一存在する. その環準同型は全射であるので, その核を I と書くと, k 上の環の同型 $R \cong k[x_1, \dots, x_m]/I$ が成立している. Hilbert の基底定理より, ある $f_1, \dots, f_M \in k[x_1, \dots, x_m]$ が存在して $I = (f_1, \dots, f_M)$ が成立する.

環の同型 $R \cong k[x_1, \dots, x_m]/I$ は直観的には, R が $k[x_1, \dots, x_m]$ の中の f_i たちを全て 0 とみなすことによって得られる環に等しいことを意味している. このことから, 可換環 R とその生成元 ξ_i の組には, 不定元 x_i たちに関する多変数連立代数方程式 $f_1 = \cdots = f_M = 0$ に対応していることがわかる. この方程式は R の生成元 ξ_i たちが満たす基本関係式である[15].

たとえば, $k[x, y]$ を $y^2 - x^3 + x$ で生成されるイデアルで割ってできる剰余環 $k[x, \sqrt{x^3 - x}]$ は $y^2 = x^3 - x$ という楕円曲線の方程式に対応している.

$k[x]/(x^3)$ は $x^3 = 0$ という方程式に対応している. 方程式 $x^3 = 0$ の体 k における解は $x = 0$ しか存在しないが, もしも $\epsilon^3 = 0$ を満たす 3 位の無限小数 ϵ が存在すれば ϵ も方程式 $x^3 = 0$ の解になっている. よって, $x = 0$ という方程式と $x^3 = 0$ という方程式を区別することには意味がある. $\epsilon \in k[x]/(x^3)$ を $\epsilon := x \bmod (x^3)$ と定めれば, ϵ は $\epsilon^3 = 0$ という基本関係式を満たしている[16].

一般論に戻ろう. $R \cong k[x_1, \dots, x_m]/I$, $I = (f_1, \dots, f_M)$ は上と同様とし, A は k 上の任意の可換環であるとする. x_i たちに関する連立代数方程式 $f_1 = \cdots = f_M = 0$ の環 A における解 $(a_1, \dots, a_m) \in A^m$ と k 上の環準同型 $\alpha : R \to A$ が自然に一対一に対応していることを説明しよう.

解 $(a_1, \dots, a_m) \in A^m$ は $f_1(a_1, \dots, a_m) = \cdots = f_M(a_1, \dots, a_m) = 0$ を満たしているので, x_i に a_i を対応させる $k[x_1, \dots, x_n]$ から A への k 上の環準同型の核は $I = (f_1, \dots, f_M)$ を含む. よって, それは ξ_i を a_i に対応させる R から A への k 上の環準同型を誘導する. 逆に, k 上の環準同型 $\alpha : R \to A$ に対して, $a_i = \alpha(\xi_i) \in A$ と置くと,

$$f_j(a_1, \dots, a_m) = f(\alpha(\xi_1), \dots, \alpha(\xi_m)) = \alpha(f(\xi_1, \dots, \xi_m)) = \alpha(0) = 0.$$

[15] それらの関係式から ξ_i たちの満たす他の関係式が全て導かれるとき, それらの関係式は ξ_i たちの基本関係式であると言う.

[16] 巾零元を含む一般の可換環も含めて代数幾何の大理論を建設したのは A. Grothendieck である.

すなわち, $(a_1, \ldots, a_m)$ は方程式 $f_1 = \ldots = f_M = 0$ の解である.

R の生成元の取り方を変えることは方程式の座標変換に対応していることを説明しよう.

R の別の生成元 $\eta_1, \ldots, \eta_n$ を取る. 上と同様に, $R \cong k[y_1, \ldots, y_n]/J$, $J = (g_1, \ldots, g_N)$, $g_j \in k[y_1, \ldots, y_n]$ が成立する. ここで, η_j たちの満たす基本関係式は $g_1 = \cdots = g_N = 0$ である.

ξ_i は η_j の多項式で書けるので, ある $\phi_1, \ldots, \phi_m \in k[y_1, \ldots, y_n]$ が存在して $\xi_i = \phi_i(\eta_1, \ldots, \eta_n)$ が成立する. 逆に, η_j は ξ_i の多項式で書けるので, ある $\psi_1, \ldots, \psi_m \in k[y_1, \ldots, y_n]$ が存在して $\eta_j = \psi_j(\xi_1, \ldots, \xi_m)$ が成立する. ϕ_i と ψ_j は座標 x_i における方程式 $f_1 = \cdots = f_M = 0$ と座標 y_j における方程式 $g_1 = \cdots = g_N = 0$ のあいだの座標変換になっている.

以上のように, 有限生成環は多変数連立代数方程式の抽象化であり, 方程式の解は環の準同型で表現でき, 方程式の座標変換は生成元の取り方を変えることで表現できることがわかった.

連立代数方程式は代数多様体の定義方程式とみなせることに注意すれば, 可換環論と代数幾何学の関係も何となくわかるだろう[17].

素数 p に対する p 進整数環 $\mathbb{Z}_p = \operatorname{proj}\lim_{n\to\infty} \mathbb{Z}/p^n\mathbb{Z}$ も重要な可換環である. $\mathbb{Z}_p$ は離散位相を入れた有限環 $\mathbb{Z}/p^n\mathbb{Z}$ の射影極限としてコンパクトな位相環をなす. p 進整数環は形式巾級数環 $k[[x]] = \operatorname{proj}\lim_{n\to\infty} k[x]/(x^n)$ に似ている[18]. k が有限体ならば $k[[x]]$ も自然にコンパクトな位相環をなす.

3.3 体にはどのようなものがあるだろうか?

$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ はおそらくもっとも身近な体であろう. この他に, 標数 p で位数 $q = p^e$ の有限体 $\mathbb{F}_q$ や p 進体 $\mathbb{Q}_p$ も基本的な体の仲間に入れておいた方が良い[19].

数学によく現われる体は以上の基本的な体の有限次拡大や代数拡大や超越次数が有限の超越拡大になっている[20].

たとえば $\mathbb{Q}$ の有限次拡大は代数体と呼ばれている[21]. 有限体上の有理函数体 $\mathbb{F}_q(x)$ の有限次拡大は有限体上の 1 変数代数函数体と呼ばれている. コンパクト Riemann 面上の有理型函数の全体のなす体はコンパクト Riemann 面の代数函数体と呼ばれており, 複素数体上の有理函数体 $\mathbb{C}(z)$ の有限次拡大体になっている. 代数体と有限体上の 1 変数代数函数体とコンパクト Riemann 面の代数函数体は似ている.

---

[17]代数多様体と可換環論の関係は可微分多様体とユークリッド空間の開集合の関係の類似になっている. 可換環論を幾何学的イメージに沿って解説した易しい入門書に M. リード著『可換環論入門』(岩波書店) [8] がある. 筆者は学部時代に可換環論の話を初めて知ったとき何をやっているのかさっぱり理解できなかった. たとえば, どうして「局所化」と言うのか? 実は可換環論は多様体論の一種なのだということを理解して初めて可換環論の様々な定理が非常に自然であることを納得できた.

[18]$k[[x]]$ は整域だが射影極限を取る途中の $k[x]/(x^n)$ は巾零元を含む. $k[[x]]$ のような環を代数幾何において役立てるためには, 巾零元を含む環をも代数幾何の対象にするのが自然である.

[19]p 進体 $\mathbb{Q}_p$ と体 k 上の形式 Laurent 級数体 $k((x))$ は似ている. $\mathbb{Q}_p$ の元は $a_0p^{-N} + a_1p^{-N+1} + a_2p^{-N+2} + \cdots$ $(a_i = 0, 1, \ldots, p-1)$ の形をしており, $k((x))$ の元は $a_0x^{-N} + a_1x^{-N+1} + a_2x^{-N+2} + \cdots$ $(a_i \in k)$ の形をしている. $\mathbb{Q}_p$ は $\mathbb{Z}_p$ の商体に等しく, $k((x))$ は $k[[x]]$ の商体に等しい. R や $\mathbb{C}$ や $\mathbb{Q}_p$ は局所コンパクトな位相体であり, k が有限体ならば $k((x))$ も自然に局所コンパクトな位相体である.

[20]より精密な言い方は次の通り. 素体 $\mathbb{F}_p, \mathbb{Q}$ から出発して, 有限次拡大する, 完備化する, n 変数有理函数体 $K(x_1, \ldots, x_n)$ を作る, という操作を有限回繰り返すことによって得られる体は数学において基本的である.

[21]代数体の全体がどのような世界をなしているかという問題はおそるべき難問である. しかし, おそるべき難問に近付く前にやっておくべきことはたくさんある. たとえば, あなたは構造がよくわかる代数体の具体例をどれだけ知っているだろうか?

一般に体 k の超越次数が有限の超越拡大 K は何を意味しているのだろうか?

K の k 上の超越次数を n とすると, K は k 上の n 変数有理函数体 $K_0 = k(x_1, \ldots, x_n)$ の有限次拡大に同型である. すなわち, K_0 上代数的な $\theta_1, \ldots, \theta_r \in K$ が存在して, $K = K_0[\theta_1, \ldots, \theta_r]$ (すなわち K は θ_i たちから K_0 上環として生成される). よって, K は K_0 上の r 変数の多項式環 $K_0[y_1, \ldots, y_r]$ を極大イデアル $\mathfrak{m} = (f_1, \ldots, f_N)$ で割ってできる体に同型である. 極大イデアル $\mathfrak{m}$ は x_i と y_j たちに関する方程式 $f_1 = \ldots = f_N = 0$ に対応している[22].

以上によって, 体 k 上の超越次数が有限の超越拡大にも連立代数方程式が対応していることがわかった[23].

たとえば, $a, b \in k$ に対して, $k[x, \sqrt{x^3 + ax + b}] = k[x, y]/(y^2 - x^3 - ax - b)$ の商体 K は k 上の楕円曲線 $y^2 = x^3 + ax + b$ に対応する楕円函数体と呼ばれている. 楕円函数体 K は $k(x)[y]$ を $y^2 - x^3 - ax - b$ で生成されるイデアル (極大になる) で割ってできる体に同型である.

以上と同様に「方程式にはどのようなものがあるだろうか?」と問うのも楽しい. 小学生のときから様々な方程式について習って来たはずだが, それらの方程式は抽象代数学の言葉でどのように表現されるのかについて考えてみよ[24].

「非可換環にはどのようなものがあるだろうか?」という問いも基本的である. 微分作用素環や群の群環や Lie 環の普遍展開環などは結合的で 1 を持つ自然な非可換環の例であり, 量子群のような新しい例もある. 微分作用素環は通常 D と書かれることが多いので, 微分作用素環上の加群の理論は D 加群の理論と呼ばれている. D 加群は線型微分方程式の抽象化である. 群環や Lie 環の普遍展開環上の加群は群や Lie 環の表現に等しい. 群や Lie 環や量子群は対称性の概念の抽象化である.

以上ではかなり足早に代数学における基本的概念の風景を眺めてみたが, 自分でやる場合にはもっとじっくりゆっくり楽しみながら色々眺めてみた方が良い.

4 セミナーでの話し方について

4.1 大きな声で明僚に話す

何よりも大きな声で明僚に話すべきである.

ゴニョゴニョと小さな声で不明瞭に話されるとものすごく感じが悪い.

---

[22] この場合においてイデアル $\mathfrak{m}$ が極大であることは, generic な x_i たちが与えられているとき, $f_1 = \ldots = f_N = 0$ を y_j たちに関する方程式だとみなせば, その解が有限個の点からなることを意味している. 図を描いてみよ.

[23] 体の有限次拡大の理論の幾何的類似は被覆の理論であり, 体の Galois 理論の幾何的類似は基本群と被覆空間の Galois 理論である. 筆者は, 学生時代に初めて体の Galois 理論について知ったとき, 何をやっているのかさっぱりわからなかった. しかし, トポロジーの言葉で展開できる基本群と被覆空間の Galois 理論は絵を描いて理解できるので何をやってるか非常にわかり易いと思った. コンパクト Riemann 面の代数函数体の Galois 理論とコンパクト Riemann 面の分岐被覆の Galois 理論が数学的に同値なので, コンパクト Riemann 面の世界では代数的な Galois 理論と幾何的な Galois 理論が統一されている. 久賀道郎著『ガロアの夢——群論と微分方程式——』(日本評論社) [1] は基本群と被覆空間からの Galois 理論入門として非常に面白い本である. なお, 『ガロアの夢』の後の方に書いてある未解決問題の一部は現在では D 加群の理論が整備されたおかげで解決している.

[24] 代数方程式に限らず, 微分方程式でさえ微分環や D 加群の言葉を用いれば代数的に定式化できる. 佐藤幹夫はそのようなアイデアを発展させた. 代数方程式だけではなく微分方程式をも含めて代数的に扱うという思想は「佐藤フィロソフィー」と呼ばれている. 佐藤フィロソフィーは線型偏微分方程式論や KdV 方程式や KP 方程式のようなソリトン方程式において大成功をおさめている.

大声を出すことは緊張をほぐすために役に立つので, 頭の回転を正常な状態に保つためにも効果がある.

個人的には大きな声で明僚に話すことは最も重要なことだと思う.

4.2 十分な準備をしておく

もちろん, 虚勢ではなしに大声を出せるだけ十分に準備しておかなければいけない.

わからないところがあっても, 何十時間も集中し, あらゆる手段を使って調べ, 考えまくって, 何百枚も計算用紙を費したのにそうだったのであれば[25], 必要な関連の知識はかなり増えているはずである. おそらく, 完全な理解にはたどり着いてなくても, 部分的な理解にはたどり着いているだろう[26].

結果的に必要な知識が何も増えないような勉強の仕方は, きっと「集中」とも無縁だろうし, 思い付く限りの「あらゆる手段」を使ってもいないだろうし, 「考えまくって」もいないに違いない.

理解に行き詰まって先に進めなくなったときには, どうすれば良いのかについて全力で考えてみるべきである. 基礎的知識が足りなければそれを補えばよい.

基本的なところから順番に積み重ねて行けばどんなに難しい数学であってもいつかは理解できるはずである. 凡人はそうやって膨大な時間をかける以外にない. 毎週のように膨大な努力を積み重ねれば必ず進歩できるはずである.

塵も積もれば山になる!

なお, セミナーで質問されるかもしれないという理由からだけではなく, なかなか理解できないことを部分的に理解するためには簡単な具体例について考察してみることが役に立つ. 一般的で難しい定理の証明をいきなり読む前に, 簡単な例でそれが実際に成立しているかを確かめておくと理解し易くなる場合が多い.

4.3 わかり易く話すように気を使う

わかり易く話すのは非常に難しい. しかし, わかり易く話すためにはどうすれば良いかについて考えたり, 努力したりすることならば今すぐにでもできるはずである.

話を聴いている人たちのことを何も考えずに話すことは, 数学に限らず, どのような場所においても好ましいことではない.

なお, 慣れないうちは変に工夫したりせずに, 地道で正確な説明を心掛けるのが良いと思う.

ただし, 地道で正確であることは, テキストに書いてあることをそのまま黒板に書くこととは違う. 場合によってはテキストの説明を完全に書き直すことが必要である. 論理的内容を保ったままでより正確でより厳密でわかり易い説明を自分で再構成するのである.

---

[25] セミナーの準備にはこの程度の努力は当然必要である.

[26] 数学に限らず, 「完全な理解がすぐにはできそうもない場合にはひとまず部分的な理解を目指してみること」は常套手段である. どのような中間目標を設定すれば完全な理解に近付くかをよく考えなければいけない. たとえば, 自分に欠けている知識を補うことを目標にしたり, 特殊な場合に成立していることをチェックしたりすることを目標にすることになる. 他にも, 類似の問題に挑戦してみて感じをつかもうとしてみたり, より一般的な問題が一挙に解けてしまわないかについて考えてみたり, 直接にその問題が解けなくてもやれることはたくさんある. 自分自身の知識を進歩させるために肝腎なことは, すぐに理解できそうもないことにぶち当たったときに何をやるかなのだと思う.

4.4 目標と結論をできるだけ早目に述べる

話を聴く立場のものにとっては, できるだけ早く目標と結論を述べてくれた方がありがたい. その理由は目標と結論が前もってはっきりしていれば, それに向けて精神を集中できるからである. 小説や映画の類でネタバレは困るが, 数学の場合はそうではない.

何が目標で何が結論なのかを何も示さないまま長くて複雑な議論に突入すると, 話を聴く方は何が大事なのかがわからなくなってしまう. 最後に結論がわかっても, 神経を集中させることができないままで聴いた話はすでに忘れてしまっていることが多い.

セミナーで話すときには, まず最初にこれから何を目標とするかをおおざっぱに述べてから始めるべきである. そして, 各議論のステップごとにその結論を先に示すようにする.

4.5 どこが面白いかがわかるように説明する

数学には感動がなければいけない. ささいなことであっても感動できることは多い.

今までよくわからなかったことについて本質がほんの少し垣間見えたときには本当に嬉しくなる.

感激できるだけの努力と理解を目指し, それに成功すれば血肉になるような進歩が得られるだろう. そういう経験は数学に限らずあらゆる分野で役に立つと思う.

参考文献

[1] 久賀道郎: 『ガロアの夢——群論と微分方程式——』, 日本評論社, 1968

[2] 佐武一郎著: 『線型代数学』, 数学選書 1, 裳華房, 1958

[3] I. R. シャファレヴィッチ: 『代数学とは何か』, 蟹江幸博訳, シュプリンガー・フェアラーク東京, 2001

[4] 日本数学会編集, 『岩波数学辞典第 3 版』, 岩波書店, 1985

[5] 堀田良之: 『代数入門——群と加群——』, 数学シリーズ, 裳華房, 1987

[6] 堀田良之: 『加群十話——代数学入門——』, すうがくぶっくす 3, 朝倉書店, 1988

[7] 森田康夫: 『代数概論』, 数学選書 9, 裳華房, 1987

[8] M. リード: 『可換環論入門』, 伊藤由佳理訳, 岩波書店, 2000