教養原論 数理の世界
数学とコンピュータ 2013 (第 1 回)

野呂 正行

神戸大学理学研究科数学専攻

October 3, 2013

0. 授業の目標

アルゴリズム, ハード, ソフトの発展により, 数の演算に限らず, 式, 図形, 論証なども可能になっている.
⇒ コンピュータに数学を「実行」させよう

- **数学を実行するアルゴリズムを学ぶ**
  (普通の) 計算機は考えることができない
  ⇒ 計算機に計算させる方法 (アルゴリズム) を学ぶ

- **計算機上で数学を実行するソフトウェアの紹介**
  有用なフリーソフトがたくさん : 代数, 解析, 幾何, 統計
  ⇒ いくつかを実際に使ってみる

  予定 : 暗号解読, 入試問題を解かせる, 幾何ソフトを使ってみる etc.

授業, 実習, 評価の方法

- **授業**

  計算方法の紹介 : 黒板を使うことが多いはず.

  数学ソフトウェアの紹介, デモ : プロジェクタで

- **実習**

  暗号解読, 初等幾何, 記号計算など

  実習は別室で行うので, 事前の予告, 掲示に注意

  授業用連絡ページは

  http://www.math.kobe-u.ac.jp/HOME/noro

- **評価**

  数回課されるレポートによる

  原則: その場で提出 (必須)

今日の授業の内容

1. **これまでに学んだ数学と計算機**
   数学を実用的につかうための計算機の必要性
2. **計算機上で実行される数学**
   現在どのような数学が計算機上でできるかの紹介
3. **計算機に適したアルゴリズム**
   計算機に計算させるには, 計算機の特性をうまく利用するアルゴリズムが必要
4. **数学ソフトウェア**
   数の計算だけではなく, 文字を含む式なども計算できるソフトウェアの紹介

1. これまで学んだ数学と計算機

例: 漸化式 $a_{n+1} = f(a_n)$

- **高校数学では**
  漸化式を「解く」, すなわち a_n を n の式で表すことが主眼だった
  $\Rightarrow$ 実際にはほとんどの漸化式は解けない

- **応用の現場では**
  $a_1, a_2, \ldots$ を次々計算するために使う.
  例 : n 次方程式の解
  漸化式によりいくらでも高精度に計算可能
  $\Rightarrow$ **計算機がないと実用上無理**

例：a 平方根 $\sqrt{a}$ の計算

かつては, 中学の教科書に, 「開平法」という複雑な方法が載っていた

$\Rightarrow$ ニュートン法を使えば簡単に高精度に計算できる.

$$a_1 = 1, \quad a_{n+1} = \frac{a_n + \frac{a}{a_n}}{2}$$

$a = 2$ の場合

$a_1 = 1$

$a_2 = 1.5$

$a_3 = 1.416$

$a_4 = 1.414215$

$a_5 = 1.414213562374$

$a_6 = 1.41421356237309504880168$

$a_7 = 1.41421356237309504880168872420969807856967187537$

これまで学んだ数学と計算機 (つづき)

例: 行列 (線形代数)

- **大学の線形代数の授業では**
  連立一次方程式の掃き出し法による解法を学ぶ
  固有値固有ベクトルの計算法を学ぶ
  $\Rightarrow$ 行列サイズはせいぜい 4 行 4 列程度

- **応用の現場では**
  いわゆる科学技術計算の大部分は行列計算
  (Google の pagerank も固有ベクトル計算)
  数万〜数百万行 (もっと大きい場合もあり) の行列が扱われる.
  $\Rightarrow$ **計算機でないと不可能**

これまで学んだ数学と計算機 (つづき)

例: 微積分

- **高校数学では**
  簡単な関数 (多項式, 指数, 対数, 三角関数) の微積分
  $\Rightarrow$ 手で計算できる程度のものばかり

- **応用の現場では**
  不定積分は計算できないのが普通
  積分は実際に細かく分割して足し合わせる (区分求積)
  $\Rightarrow$ **計算機でないと不可能**

計算機による微積分 (Maple)

Maple：大学の端末で誰でも使える数学ソフト

- **微分** $f'(x)$, $f''(x)$, $\frac{\partial^4 f}{\partial x^2 \partial y^2}$

  `diff(f,x)`, `diff(f(x),x,x)`, `diff(f,x,x,y,y)`

- **(不定) 積分** $\int f(x)dx$

  `int(f,x)`

```
f:=diff(log(sqrt((1-cos(x))/(1+cos(x)))),x);

                          ...

g:=simplify(f);
                            1
                         --------
                         sin(x)

h:=int(g,x);
                    ln(csc(x)-cot(x))
```

数学は役に立つのか?

「私は二次方程式もろくにできないど, 65 歳になる今日まで全然不自由しなかった」(ある小説家)
「. . . という委員を半分以上加えて数学教育の内容の見直しを行う必要がある」(教育課程審議会会長)
(「数学, この大いなる流れ」でググれ) ⇒ ゆとり教育へ

- **これまで学んだ数学**
  社会の要請により生まれ, どこかで役に立っている
  あらゆる理工系の学問における共通言語として必須

- **(ちなみに) その先にある数学**
  学問としての数学 : 社会の役に立つかどうかより, 学問的価値を信じて研究している
  ⇒ 結果として, 応用が生じる場合もある

  例 : 数論応用暗号 (RSA, **楕円曲線暗号** etc.)

計算機, ソフトウェアの必要性

「社会の要請」に応えるには計算機が必要

- **計算機 (ハードウェア) の必要性**
  例 : 微積分, 線形代数は理工学における基本ツール
  高校までの数学+α で内容的には十分
  しかし, 現実の問題を解くには, 紙とエンピツでは間に合わない (規模の問題)
  $\Rightarrow$ **高速, 大容量の計算機**が必要

- **ソフトウェアの必要性**
  計算機自体が提供する命令はごく単純なもののみ
  $\Rightarrow$ それらを組み合わせて複雑な処理を実行するための**ソフトウェア**が必要

計算機は PC で十分

- **かつては大型計算機が必要だった**
  ミサイル, ロケットの弾道計算 etc.
  (微分方程式の数値計算 $\Rightarrow$ 差分化, 固有値計算等)
- **スーパーコンピュータは必要ない?**
  現在のスーパーコンピュータ : 特殊な大規模計算を行うためのもの
- **ふつうの数学には PC で十分**
  実は, PC でも一昔前のスーパーコン並の性能
  PC 上で数学を実行できるソフトウェアがたくさんある

2. 計算機上で行われる数学の例

- **数値計算 : 浮動小数を基礎とした計算**
  大規模行列計算 (線形代数), 微分方程式の数値解法, . . .
- **代数的計算 (この授業ではこれを主として解説)**
  - **数の演算**
    整数, 有理数, 有限体, 平方根 . . .
    電卓と違い, 任意の大きさの数, 任意精度の数を扱う
  - **式の演算**
    展開, 因数分解, 方程式求解, 微分, 積分 . . .
- **可視化** (visualization)
  数学的な図形をディスプレイ上に表示
  ⇒ 数式からは分からないことが直観的に理解できる
- **不等式の計算**
  工学的応用 (最適化) を目的とするが, 大学入試問題も解いてしまう

分数, 小数の計算

- **浮動小数**

  例 : 1.23×10^5 (1.23 : **仮数部**, 10^5 : **指数部**)

  計算機で数といえば普通はこれを指す (電卓でも同様)

  仮数部 : **せいぜい** 10〜15 **桁**

  ⇒ **計算しているうちに誤差が入る**

  例 : $1/3 \times 3$ **が** $0.999\cdots9$

  ⇒ **これでは数学を厳密にやるのは困難**

- **有理数**

  計算機ハードは有理数を扱ってくれない

  ⇒ **有理数 (いくらでも大きい数) を厳密に扱うには, アルゴリズム (プログラム) が必要 (多倍長演算**, GCD)

  ⇒ **既にいろいろなソフトで実現されている**

  フリーソフト gmp : **いろいろなソフトに組み込まれて使われている**

有限体

例：5 **元体** $\mathbf{F}_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$

$\bar{x}$ **は**, 5 **で割った余り** $\Rightarrow \mathbf{F}_5$ **は** 5 **で割った余りの集合**

加減乗算：**ふつうに計算して** 5 **で割った余りをとる**

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$

$\times$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

除算：$\bar{a} \neq \bar{0}$ **なら** $\bar{a} \times \bar{b} = \bar{1}$ **となる** $\bar{b}$ **がある** $\Rightarrow$ **除算ができる**

用途：**暗号** (RSA, **楕円曲線**), CD/DVD **エラー訂正**, **近似計算**

多項式演算

- **多項式の計算機上での表現**
  例：$2x^3 - x + 2 \Leftrightarrow (x, ((3, 2), (1, -1), (0, 2)))$
  $\Rightarrow$ **構造を持つデータも, 最終的には数を使って表現できる**

- **因数分解**
  - **人間のやり方：眼力法**
    せいぜい 3, 4 **次まで (係数が大きいとアウト)**
  - **計算機で使うアルゴリズム：有限体の利用**
    全く違う方法. 1000 **次でも, 巨大係数でも** OK.

多項式因数分解

例 $f(x) = x^2 + x - 2$

- **人間 : かけて** -2**, 足して** 1
  次数が上がる, 係数が大きくなるとお手上げ

- **計算機 : 有限体による近似**
  $f(x) - (x+2)(x+4)$ **が** 5 **で割り切れる**
  $f(x) - (x+2)(x+24)$ **が** $5^2 = 25$ **で割り切れる**
  $f(x) - (x+2)(x+124)$ **が** $5^3 = 125$ **で割り切れる**
  $\cdots$
  k **を十分大きくとり, 整数上に引き戻して本当に割り切れるかどうか調べる**
  $(124 > \frac{125}{2}$ **から** $124 \to 124 - 125 = -1$ **として**

$$(x+2)(x-1) = x^2 + x - 2$$

となり, $f(x)$ **が分解できた)**

多項式演算の例 (Risa/Asir)

```
[1833] F=x^32+8*x^28+20*x^24+2632*x^20-30490*x^16
+74872*x^12+23316*x^8+14904*x^4+1;
x^32+8*x^28+20*x^24+2632*x^20-30490*x^16+74872*x^12
+23316*x^8+14904*x^4+1
0sec(1.001e-05sec)
[1834] fctr(F);
[[1,1],[x^16+4*x^12-16*x^11+80*x^9+2*x^8+160*x^7
+128*x^6-160*x^5+28*x^4-48*x^3+128*x^2-16*x+1,1],
[x^16+4*x^12+16*x^11-80*x^9+2*x^8-160*x^7+128*x^6
+160*x^5+28*x^4+48*x^3+128*x^2+16*x+1,1]]
0sec(0.000699sec)
```

方程式求解

数値計算による方程式求解：大規模問題が扱えるが近似解
代数的方法：大規模問題は無理だが, 厳密解が得られる

- **連立一次方程式**
  - 人間：なんらかの消去法
  - 計算機：基本は人間と同じだが, 行列により巨大な方程式も扱える
- **連立高次方程式** (2 次以上の項を含む方程式)
  - 人間：消去法が基本だが, 方針が立ちにくい
  - 計算機：アルゴリズムにより相当複雑なものが自動的に解ける

微積分

初等関数 (多項式, 有理式, 指数, 対数, 三角関数など) については人間も計算機もアルゴリズムで計算できる

- **微分**
  - **基本的関数の公式**
    $x' = 1, (e^x)' = e^x, (\log x)' = \frac{1}{x}, (\sin x)' = \cos x$ etc.
  - **線形性** : $(af + bg)' = af' + bg'$
  - **積の微分** : $(fg)' = f'g + fg'$
  - chain rule : $f(g(x))' = f'(g(x))g'(x)$
- **不定積分**
  - **人間** : **部分積分**, **置換積分による試行錯誤**
  - **計算機** : **人間が実行できそうもない複雑なアルゴリズム**

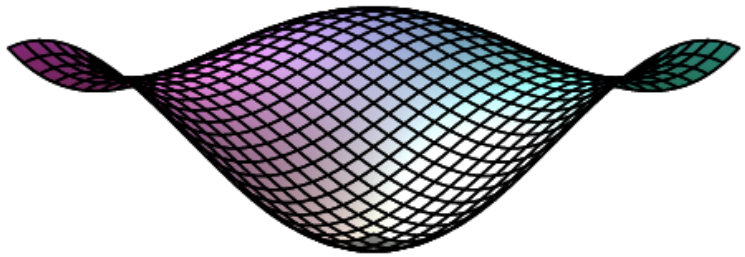
可視化 : グラフ描画

- $y = f(x)$ (**例** : $y = \sin x + \sin 2x$)
- $z = f(x, y)$ (**例** : $z = x^2 - y^2$)
  人間と同じ : 細かくプロットしてつなぐ
- $f(x, y) = 0$ (**曲線**) $f(x, y, z) = 0$ (**曲面**)
  曲線の例 : $x^3 + xy + y^3 - 1 = 0$
  曲面の例 :
  $16zx^4 - 4y^2x^3 - 128z^2x^2 + 144zy^2x - 27y^4 + 256z^3 = 0$
  - **人間** : $y = g(x), z = g(x, y)$ **と解けないとつらい**
  - **計算機 : いろいろ難しいことをやって描く**

2 変数関数のグラフ (Maple)

```
plot3d(f,x=a..b,y=c..d)
```

```
plot3d(x^3+y^3-3*x*y,x=-5..5,y=-5..5);
```



可視化：初等幾何

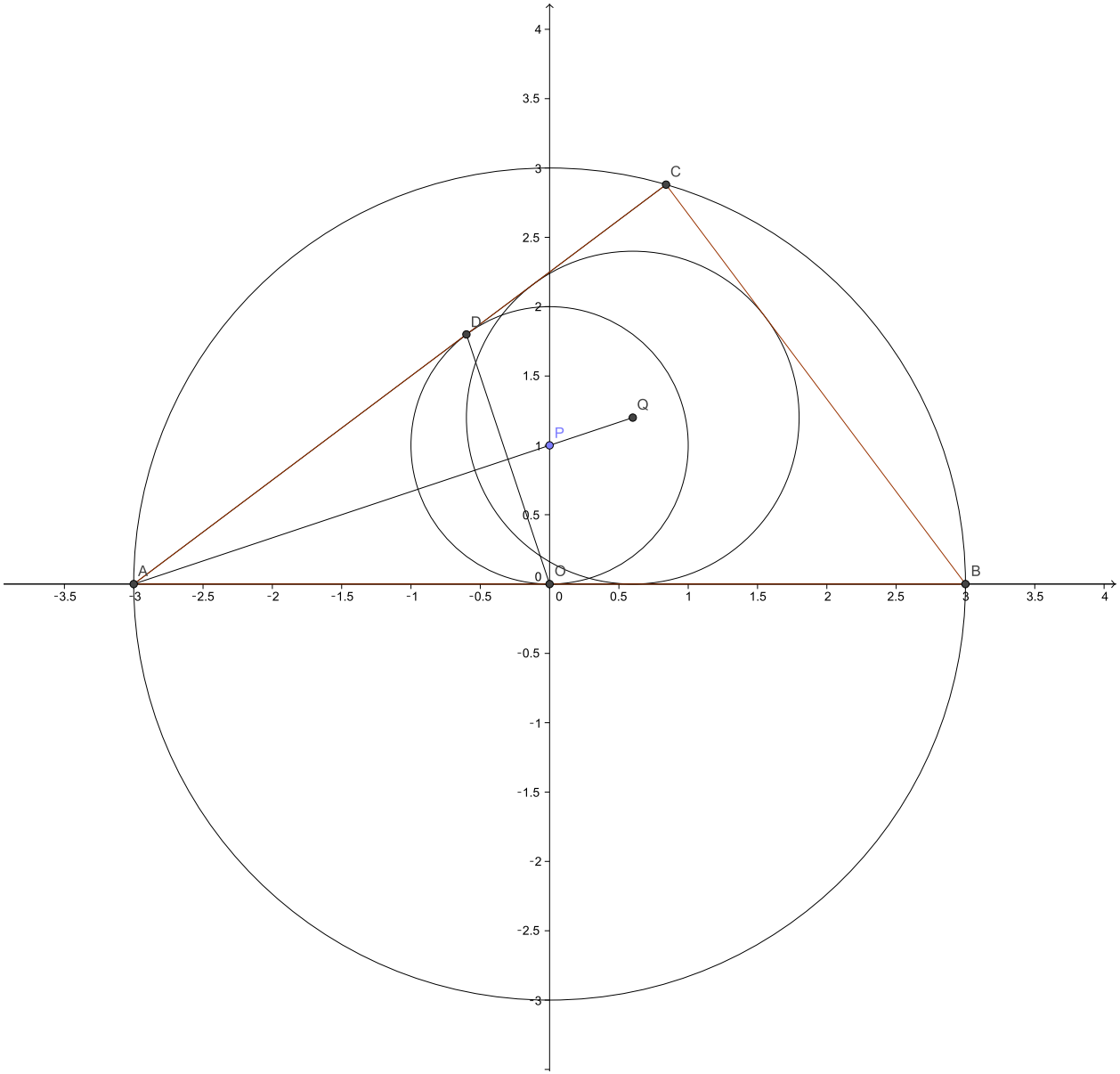
初等幾何：**円**, **直線**, **三角形** etc.
いろいろな定理がある (**例**：**三角形の各辺の垂直二等分線は一点で交わる**)
⇒ **これを目で見て**, **図を動かしながら確かめられるソフトがいくつかある**

例：KSEG, GeoGebra, KidsCindy (**日本製**)

例：GeoGebra

- GeoGebra = Geometry (**幾何**) + Algebra (**代数**)
  幾何, 代数 微積分を結びつけた数学ソフトウェア
  学校で使うことを目的に作られている
- **ウェブから簡単に起動できる.**
  Java **が入っていれば** Windows, Macintosh, Linux **上どこでも** OK. (**今日は** Linux (KNOPPIX/Math) **上で使用**.)
- **図形, グラフが簡単に描ける**
  描かれた図形の移動, 変形も容易
- **パラメタに依存するグラフが書ける.**
  スライダーを使ってグラフを変形できる.
- **簡単な数式の計算ができる.**
  多項式, 指数、対数, 三角関数, 微分, 積分 . . .

とある入試問題 (GeoGebra)



3. 計算機に向いたアルゴリズムも学ぶ

- 人間が行う計算
  - 思いつき, ひらめきの援用
  - 単純かつ長い繰り返しは苦手
- 計算機
  - 思いつく, ひらめくは無理.
  - 単純な計算を言われた通りにしかできない.
  - 長い繰り返しも嫌がらずにやる. (人間と逆)

$\Rightarrow$ この特性を生かしたアルゴリズムがたくさんある
ソフトの使い方だけでなく, 中身についても少し学ぼう

計算機向きのアルゴリズム例：線形代数

- **行列の積**

  $n \times n$ 行列 A, B の積：かけ算が n^3 回必要

  $\Rightarrow n$ が大きいと人間がやれる計算ではなくなる

  計算自体は単純な繰り返しなので，計算機向き

- **連立一次方程式の求解** ($Ax = b$ を満たす x を求める)

  ガウス消去：これも n^3 の手間が必要

  これも計算機向き

- **互除法**

  $a = q_1 b + r, b = q_2 r + r', r = q_3 r' + r'', \ldots, r^{(n-1)} = q_n r^{(n-2)}$

  $\Rightarrow \mathrm{GCD}(a, b) = r^{(n-2)}$

  余りを余りで割った余り??? でも，素因数分解より圧倒的に高速

例：整数の積

$(a_{n-1}a_{n-2}\cdots a_0)_{10} \times (b_{m-1}b_{m-2}\cdots b_0)_{10}$

- **普通の方法：筆算**
  これ自体計算機向き：一桁のかけ算が mn 回必要

- **多項式の積を経由して高速化**
  $f(x) = a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,$
  $g(x) = b_{m-1}x^{m-1} + \cdots + b_1 x + b_0$
  とおき，$h(x) = f(x)g(x)$ を作れば $h(10)$ が積の値
  理由：n 次式の積を $Cn\log n$ の手間で計算できる
  $\Rightarrow$ **n が大きいと** $n^2 >> Cn\log n$

4. 数学ソフトウェア

- **商用ソフトウェア** : Mathematica, Maple
  Maple : **大学の端末で誰でも使える**
  高価で機能豊富だが必ずしも高性能とはいえない
  中身はブラックボックス
  ⇒ **結果を論文に書く場合注意が必要**

- **フリーソフトウェア**
  大抵は研究者が自分用に作ったもの (専門家向け)
  ⇒ **大勢の人に使ってもらいたいのでフリーで配布**
  オープンソースのものが多い
  ⇒ **高信頼性, みんなで改良できる**
  残念ながら, 大学の計算機 (Macintosh) **で使えるものは少ない**
  Windows, Linux **上で使えるものは大量にある**

数学ソフトウェアの利用

- Maple (**大学内で利用**)
  大学全体でサイトライセンスを取得 ⇒ 大学内で自由に使える
  白い Mac **にログインすると**, Maple **のアイコンが** dock **にあるはず**.
  微積分の勉強なら Student[Calculus1] **パッケージを使ってみる**
  (**ヘルプ** → Calculus1 **を検索**)
- Maxima (**自宅で利用**)
  Maxima **はフリーソフト** (**かつては有料**; 100 **万円以上**)
  sourceforge **から取得できる** (**ググれば見つかる**)
  Maxima **入門用ノート** (**中川義行著**) **がお勧め**

ご参考：KNOPPIX/Math プロジェクト

- KNOPPIX
  Klaus Knopper (ドイツ) が作成, 配布している Live Linux CD/DVD
  Live Linux : Windows PC に CD/DVD をセットし再起動すると, 別の OS (Linux) が起動 (Windows の HDD には影響なし)

- KNOPPIX/Math
  濱田 (福岡大), 高山, 野呂 (神戸大) らが KNOPPIX 上に数学ソフトを多数追加した DVD を作成, 配布
  USB にインストールして起動できる (便利)
  Windows, Mac 上の仮想マシンとしても使える (便利)

次回以降の予定

1. 整数の四則, 互除法
2. 有限体, RSA 暗号とその解読
3. 論理の初歩と QE による不等式 (入試問題) の求解
4. 方程式とニュートン法
5. 線形代数
6. 初等幾何, グラフ描画

などについて, 数学ソフトの紹介, 実習を織り交ぜながら進めていく.

講義資料等 : http://www.math.kobe-u.ac.jp/HOME/noro