Chapter 2- § 4
割り算のアルゴリズム

- $k[x,y,z\ldots]$に対する割り算の定式化

$$f \in k[x_1, \cdots, x_n] \quad f_1, \cdots, f_s \in k[x_1, \cdots, x_n]$$

$$f = a_1 f_1 + \cdots + a_s f_s + r$$

- a_1, a_2,.... : 商（quotients）
- r : 余り（remainder）

例1

- $x > y$のlex順序

$$f = xy^2 + 1$$

$$f_1 = xy + 1 \quad \mathrm{LT}(f_1) = xy$$

$$f_2 = y + 1 \quad \mathrm{LT}(f_2) = y$$

$$\text{商}\left\{\begin{array}{l} a_1 : \\ a_2 : \end{array}\right.$$

$$\begin{array}{r} xy+1 \\ y+1 \end{array} \;\sqrt{xy^2+1}$$

先頭項 $\mathrm{LT}(f_1) = xy$ と $\mathrm{LT}(f_2) = y$ の両方で $\mathrm{LT}(f) = xy^2$ を割る.

$$\begin{array}{ll} a_1 : & y \\ a_2 : & \end{array}$$

$$\begin{array}{r} xy+1 \\ y+1 \end{array} \;\sqrt{\begin{array}{r} xy^2+1 \\ xy^2+y \\ \hline -y+1 \end{array}}$$

次に，同じ計算プロセスを $-y+1$ に対して行う．今度は，$\mathrm{LT}(f_1) = xy$ は $\mathrm{LT}(-y+1) = -y$ を割ることはできないから，f_2 を使わなければならない．

$$
\begin{array}{rl}
a_1: & \quad y \\
a_2: & \quad -1 \\
xy+1 & \multicolumn{1}{|l}{\overline{\;xy^2+1\;}} \\
y+1 & \multicolumn{1}{|l}{\;xy^2+y} \\
\hline
 & \qquad -y+1 \\
 & \qquad -y-1 \\
\hline
 & \qquad\qquad 2
\end{array}
$$

$$
xy^2+1 = y\cdot(xy+1) + (-1)\cdot(y+1) + 2.
$$

例2

- $x > y$のlex順序

$$f = x^2y + xy^2 + y^2$$

$$f_1 = xy - 1$$

$$f_2 = y^2 - 1$$

最初にfをf_1で割る

$a_1 : \quad x + y$

$a_2 :$

$$
\begin{array}{r|l}
xy - 1 & x^2y + xy^2 + y^2 \\
y^2 - 1 & x^2y - x \\
\hline
 & \quad\quad xy^2 + x + y^2 \\
 & \quad\quad xy^2 - y \\
\hline
 & \quad\quad\quad\quad x + y^2 + y
\end{array}
$$

$$\mathrm{LT}(x+y^2+y)=x$$

$\mathrm{LT}(f_1)=xy$ と $\mathrm{LT}(f_2)=y^2$ では割れない

$$
\begin{array}{llll}
a_1 : & x+y & & \\
a_2 : & & & r \\
 & & & \overline{} \\
xy-1 & \multicolumn{1}{|l}{x^2y+xy^2+y^2} & & \\
y^2-1 & \multicolumn{1}{|l}{x^2y-x} & & \\
 & \overline{xy^2+x+y^2} & & \\
 & xy^2-y & & \\
 & \overline{x+y^2+y} & & \\
 & \overline{y^2+y} & \longrightarrow & x
\end{array}
$$

このxを余りとして処理

$$x^2y+xy^2+y^2=(x+y)\cdot(xy-1)+1\cdot(y^2-1)+x+y+1.$$

余りのどの項も除数の先頭項で割り切れてはいけない.

定理3

定理 3 ($k[x_1, \ldots, x_n]$ における割り算アルゴリズム) $\mathbb{Z}^n_{\geq 0}$ における単項式順序 $>$ を 1 つ固定し，$F = (f_1, \ldots, f_s)$ を $k[x_1, \ldots, x_n]$ の順序付けられた s 個の多項式の組とする．このとき，どんな $f \in k[x_1, \ldots, x_n]$ も

$$f = a_1 f_1 + a_2 f_2 + \cdots + a_s f_s + r$$

と，$a_i, r \in k[x_1, \ldots, x_n]$ を使って書ける．しかも，r は 0 であるか，または単項式の k 係数の線型結合で，どの単項式も $\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s)$ のいずれでも割り切れない．この r を，f を F で割った余り (remainder) と呼ぶ．さらに，もし $a_i f_i \neq 0$ であるならば，

$$\mathrm{multideg}(f) \geq \mathrm{multideg}(a_i f_i)$$

である．

アルゴリズム

Input: $f_1, \ldots, f_s, f$

Output: $a_1, \ldots, a_s, r$

$a_1 := 0; \ldots ; a_s := 0; r := 0$

$p := f$

WHILE $p \neq 0$ DO

  $i := 1$

  divisionoccurred := false

  WHILE $i \leq s$ AND divisionoccurred = false DO

    IF $\mathrm{LT}(f_i)$ divides $\mathrm{LT}(p)$ THEN

      $a_i := a_i + \mathrm{LT}(p)/\mathrm{LT}(f_i)$

      $p := p - (\mathrm{LT}(p)/\mathrm{LT}(f_i))f_i$

      divisionoccured := true

    ELSE

      $i = i + 1$

  IF divisionoccured := false THEN

    $r := r + \mathrm{LT}(p)$

    $p := p - \mathrm{LT}(p)$

例4

- fを割る$f_1, f_2, \ldots$の順序が重要である

$$f = x^2y + xy^2 + y^2$$

$$\left.\begin{aligned} f_1 &= y^2 - 1 \\ f_2 &= xy - 1 \end{aligned}\right\} \text{順番が例2と逆}$$

$$x^2y + xy^2 + y^2 = (x+1)\cdot(y^2-1) + x\cdot(xy-1) + 2x + 1$$

$$\neq$$

$$x^2y + xy^2 + y^2 = (x+y)\cdot(xy-1) + 1\cdot(y^2-1) + x + y + 1.$$

イデアル所属問題

- $f_1, f_2, \cdots \in k[x_1, \cdots, x_n]$ に対して，

$f \in k[x_1, \cdots, x_n]$ がイデアルに含まれるかどうかの判定

$$f = a_1 f_1 + \cdots + a_s f_s$$

$$f \in \langle f_1, \cdots, f_s \rangle$$

r = 0は f がイデアルに所属するための十分条件である.

イデアル所属問題

例 5 $f_1 = xy + 1, f_2 = y^2 - 1 \in k[x, y]$ とおき，変数の順序は lex 順序とする．$f = xy^2 - x$ を $F = (f_1, f_2)$ で割ると，結果は

$$xy^2 - x = y \cdot (xy + 1) + 0 \cdot (y^2 - 1) + (-x - y)$$

となる．$F = (f_2, f_1)$ に対しては

$$xy^2 - x = x \cdot (y^2 - 1) + 0 \cdot (xy + 1) + 0$$

- この例から，$r = 0$ は f がイデアルに所属するための必要条件とはなっていない

イデアル所属問題

- $f_1, f_2, f_3, \ldots$が生成するイデアルIを考える
- Iの”良い”生成元の集合が存在するかもしれない
  - 良い生成元で割ったあまりは一意に決まる
  - $r = 0$の条件がイデアル所属の必要十分条件となる

- グレブナ基底がこのような“良い”条件を持つ

おまけ

SAGE (www.sagemath.org)

System for **A**lgebra and **G**eometry **E**xperimentation

- 完全フリー，Webベースの数式処理システム
- Pythonで色々なソフトを糊付け

Mathematics packages contained in Sage[22]

Algebra	GAP, Maxima, Singular
Algebraic geometry	Singular
Arbitrary precision arithmetic	MPIR, MPFR, MPFI, NTL, mpmath
Arithmetic geometry	PARI/GP, NTL, mwrank, ecm
Calculus	Maxima, SymPy, GiNaC
Combinatorics	Symmetrica, Sage-Combinat
Linear algebra	ATLAS, BLAS, LAPACK, NumPy, LinBox, IML, GSL
Graph theory	NetworkX
Group theory	GAP
Numerical computation	GSL, SciPy, NumPy, ATLAS
Number theory	PARI/GP, FLINT, NTL
Statistical computing	R, SciPy

- Sage cell server
  - http://aleph.sagemath.org/
  - アカウント不要
  - 保存不可
- Sage note book
  - http://www.sagenb.org/
  - アカウント必要
    - Google, Yahoo等のアカウントでLogin可能
  - 保存可能

環

体(有理数)

```
R=PolynomialRing(QQ,'x,y,z')
x,y,z=R.gens()
I=ideal(x+y+z,x^2+y^2+z^2+2*x+3*y)
I.groebner_basis()

R=PolynomialRing(QQ,'x,y')
x,y=R.gens()
f=x^3-y^3
g=x-y
f.gcd(g)
```

Quick Reference : http://wiki.sagemath.org/quickref/