グレブナー基底による多項式の分解

BV18051　千葉龍朗

2020 年 6 月 12 日

目次

1　はじめに

グレブナー基底の性質の一つとして, 多項式をグレブナー基底で割り算を行うと余りは一つしかない. この性質を使った剰余環について研究を行った.

2　例

多項式環 $K[x,y]$ のイデアル I の生成元が $x+y-3$, $x-y+1$ のとき, $G=\{x-1,y-2\}$ は I のグレブナー基底の一つであるが, $f=x^2+3y^2-xy+5$ を G で割ると, $g_1=x-1$, $g_2=y-2$ としたら $f=(x-y+1)g_1+(3y+5)g_2+16$, $g_1=y-2$, $g_2=x-1$ としたら $f=(3y-x+6)g_1+(x-1)g_2+16$ となり, 確かに一致している.

3　多項式の余り

まず, 多項式をグレブナー基底で割るということについて定義する. なお, 以下の議論では $X=\{x_1,x_2,...,x_n\}$ は n 個の変数, $K[X]$ は多項式環, I は $K[X]$ のイデアル, $<$ は $K[X]$ の単項式順序, $\mathcal{G}=\{g_1,g_2,...,g_s\}$ は I と $<$ によって定まるグレブナー基底とする

定義 3.1. $f\in K[X]$ を $\mathcal{G}=\{g_1,g_2,...,g_s\}$ で割るとは, $f=p_1g_1+p_2g_2+\cdots+p_sg_s+r$ とかくことである. ただし, $p_1,p_2,...,p_s,r\in K[X]$ かつ r はどの g_i の倍数ではない多項式である. このとき, r は割った余りという.

ちなみに, r は p_i の値によらないので, これは well-defined である.

定義 3.2. 多項式環 $K[X]$ のイデアル I と単項式順序 $<$ に対し, グレブナー基底を $\mathcal{G}=\{g_1,g_2,...,g_s\}$ とする. このとき, $f\in K[X]$ と $g\in K[X]$ が合同であるとは, f, g を $\mathcal{G}$ で割ったときに余りが一致するときにいい, $f\equiv g$ とかく.

例 3.1. 先の例でいうと, $x^2+3y^2-xy+5\equiv x^3+x^2y+y+11$ である. 実際, $x^2+3y^2-xy+5=(x-y+1)(x-1)+(3y+5)(y-2)+16$, $x^3+x^2y+y+11=(x^2+xy+x+y+1)(x-1)+2(y-2)+16$ である.

これより, 多項式を割った余りによって多項式を分解できそうだが, 例えば余りが 1, 余りが 2 というように, 完全に一致する場合のみとすると無限に考える必要がある. これを避けるために以下の条件を設ける.

定義 3.3. $f,g\in K[X]$ において, 余りをそれぞれ $r_f=c_{1f}x_{1f}+c_{2f}x_{2f}+\cdots c_{tf}x_{tf}$, $r_g=c_{1g}x_{1g}+c_{2g}x_{2g}+\cdots c_{tg}x_{tg}\quad(c_{if},c_{ig}\in\mathbb{R})$ とする. ただし, これらは降べきの順に並んでいるものとする. このとき, 0 でない c_{nf}, c_{mg} において $n=m$ かつ $x_{nf}=x_{ng}$ がつねに成り立つ場合, $f\equiv g$ とする.

要するに, 2 つの多項式の余りが 4 と 17 だった場合, その 2 つは合同とみなすということである. これより, 余りの種類がある程度少なくなる. 例えば, グレブナー基底が $\{x^3-1, y^2-2\}$ だった場合, 余りは $\{0, C, x, y, x^2, xy, x^2y\}$ で生成されることが予想できる.

ここで 1 つ問題なのが, x^2 と x^2-1 を区別するかというここである. 区別の有無によっては余りがたくさんでてしまうのでとりあえず区別しない方向でいく. また, $\mathbb{Z}/6\mathbb{Z} \simeq \mathbb{Z}2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ みたいなことをしたいので, 群論と同じようなことをしていく.

4 多項式環の剰余環

まず, 議論を簡単にするために, 以下の記号を導入する.

定義 4.1. $[f]_{\mathcal{G}} = \{g \in K[X] | g \text{ を } \mathcal{G} \text{ で割った時の余りが } f\}$
$\mathcal{G}$ が明らかなときは単に $[f]$ とかく.

ここで, 先ほどの「区別しない」ということを理論的にいう.

定義 4.2. $f, g \in K[X]$ とする. このとき, $f \equiv g$ とは, f と g を $\mathcal{G}$ で割った余りをそれぞれ r_f, r_g としたとき, $\mathrm{in}_<(r_f) = \mathrm{in}_<(r_g)$ となるときにいう.

定理 4.3. 次が成立する.

$$f \equiv g, f' \equiv g' \text{なら } f + f' \equiv g + g', ff \equiv gg$$

これを示すため, 次の補題を示しておく.

補題 4.4. $\mathrm{in}_<(fg) = \mathrm{in}_<(f)\mathrm{in}_<(g)$

証明 $f = \mathrm{in}_<(f) + f'$, $g = \mathrm{in}_<(g) + g'$ とかけるので,

$$\begin{aligned}\mathrm{in}_<(fg) &= \mathrm{in}_<((\mathrm{in}_<(f) + f')(\mathrm{in}_<(g) + g')) \\ &= \mathrm{in}_<((\mathrm{in}_<(f)\mathrm{in}_<(g) + \mathrm{in}_<(f)g' + \mathrm{in}_<(g)f' + f'g'))\end{aligned}$$

ここで, $\mathrm{in}_<(f) > \mathrm{in}_<(f')$, $\mathrm{in}_<(g) > \mathrm{in}_<(g')$ なので

$$\mathrm{in}_<(fg) = \mathrm{in}_<(\mathrm{in}_<(f)\mathrm{in}_<(g)) = \mathrm{in}_<(f)\mathrm{in}_<(g)$$

□

定理 4.3 の証明

$f + f' \equiv g + g'$ について

$f+f' = f_1g_1+\cdots+f_sg_s+r_f+f'_1g_1+\cdots f'_sg_s+r_{f'}$ とかけるので, $\mathrm{in}_<(f+f') = \mathrm{in}_<(r_f+r_{f'})$ である. 同様にして, $\mathrm{in}_<(g+g') = \mathrm{in}_<(r_g+r_{g'})$ である. もし $\mathrm{in}_<(r_f) = \mathrm{in}_<(r_{f'})$ なら仮定より $\mathrm{in}_<(r_f) = \mathrm{in}_<(r_g) = \mathrm{in}_<(r_{g'})$ なので $\mathrm{in}_<(f+f') = \mathrm{in}_<(g+g')$ である. $\mathrm{in}_<(r_f) \neq \mathrm{in}_<(r_{f'})$ なら大きいほうを r としたら, 仮定より $\mathrm{in}_<(r_g)$ と $\mathrm{in}_<(r_{g'})$ の大きいほうも r となるので, $\mathrm{in}_<(f+f') = \mathrm{in}_<(g+g')$ である. よって $f + f' \equiv g + g'$.

$ff' \equiv gg'$ について

$$ff' = (f_1g_1 + \cdots + f_sg_s + r_f)(f'_1g_1 + \cdots f'_sg_s + r_{f'}) = (f_1g_1 + \cdots + f_sg_s + r_f)f'$$
$$= f_1f'g_1 + f_2f'g_2 + \cdots + f_sf'g_s + r_ff'_1g_1 + r_ff'_2g_2 + \cdots + r_ff'_sg_s + r_fr'_f$$

これより, $ff' \in [\mathrm{in}_<(r_fr_{f'})]$ である. 同様に, $gg \in [\mathrm{in}_<(r_g)r_{g'}]$ である. ここで, 補題より $\mathrm{in}_<(r_fr_{f'}) = \mathrm{in}_<(r_f)\mathrm{in}_<(r_{f'})$, $\mathrm{in}_<(r_gr_{g'}) = \mathrm{in}_<(r_g)\mathrm{in}_<(r_{g'})$ である. 仮定より, $\mathrm{in}_<(r_f) = \mathrm{in}_<(r_g)$, $\mathrm{in}_<(r_{f'}) = \mathrm{in}_<(r_{g'})$ より $\mathrm{in}_<(r_f)\mathrm{in}_<(r_{f'}) = \mathrm{in}_<(r_g)\mathrm{in}_<(r_{g'})$. よって $ff' \equiv gg'$.

□

また, 次のことがすぐにわかる.

定理 4.5. ” $\equiv$ ” は同値関係である.

これらのことにより, 多項式環 $K[X]$ をグレブナー基底 $\mathcal{G}$ で分解のようなものができる. つまり, 余りが x の集まり, 余りが y^2 の集まり, というふうに分けられる. これはそれぞれ $[x]$, $[y^2]$ と表すことができ, これらの集まりを $K[X]/\mathcal{G} = \{[f]|f \in K[X]\}$ とかくことにする. これは環論において剰余環とよばれる. これが和と積で環になっているかを調べよう.

命題 4.1. $K[X]/\mathcal{G}$ は次で定義される演算で環となる.

(1) $[f] + [g] = [f + g]$
(2) $[f][g] = [fg]$

注意 4.1. (1) は, $f + g$ を $\mathcal{G}$ で割ったときの余りのイニシャルイデアルなので実際は単項式になる.

この演算が well-defined かどうか調べる. つまり, $[a] = [c]$, $[b] = [d]$ のときに $[a + b] = [c + d]$, $[ab] = [cd]$ かどうかを調べる.

(1) について

$\mathrm{in}_<(a) = \mathrm{in}_<(b)$ なら明らか. $\mathrm{in}_<(a) \neq \mathrm{in}_<(b)$ の場合を考える. つまり, どちらか一方がもう一方より大きいので, それを p とする. このとき, $[a + b] = [p]$. ここで, $[a] = [c]$, $[b] = [d]$ より, $[c]$ と $[d]$ のどちらかは $[p]$ なので, $[c + d] = [p]$.

(2) について

仮定より, $\mathrm{in}_<(a) = \mathrm{in}_<(c)$, $\mathrm{in}_<(b) = \mathrm{in}_<(d)$ なので, $\mathrm{in}_<(ab) = \mathrm{in}_<(a)\mathrm{in}_<(b) = \mathrm{in}_<(c)\mathrm{in}_<(d) = \mathrm{in}_<(cd)$. よって $[ab] = [cd]$.

以上より, $K[X]/\mathcal{G}$ は環となることが分かった. ここからは, $\mathbb{Z}/6\mathbb{Z} \simeq \mathbb{Z}2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ のようなことを実際にしていく.

まず, I_1, I_2 を多項式環 $K[X]$ のイデアル, $\mathcal{G}_\alpha = \{g_{1\alpha}, g_{2\alpha}, ..., g_{s\alpha}\}$, $\mathcal{G}_\beta = \{g_{1\beta}, g_{2\beta}, ..., g_{t\beta}\}$ をイデアル I_1, I_2 と単項式順序 $<$ で定まるグレブナー基底とする. このとき, 集合 $K[X]/\mathcal{G}_\alpha \times K[X]/\mathcal{G}_\beta$ の演算を次のように定義する.

$$(a_1, a_2), (b_1, b_2) \in K[X]/\mathcal{G}_\alpha \times K[X]/\mathcal{G}_\beta \text{とする.}$$
$$(a_1, a_2)+(b_1, b_2) = (a_1 + b_1, a_2 + b_2), (a_1, a_2) \cdot (b_1, b_2) = (a_1b_1, a_2b_2)$$

手順として, まず写像 $U : K[X] \to K[X]/\mathcal{G}_\alpha \times K[X]/\mathcal{G}_\beta, \quad f \mapsto ([f]_{\mathcal{G}_\alpha}, [f]_{\mathcal{G}_\beta})$ が準同型写像であることを示す. そこから U の像と核を求め, $\mathcal{G}_\alpha$ と $\mathcal{G}_\beta$ の組み合わせの条件の検証を行う.

$U : K[X] \to K[X]/\mathcal{G}_\alpha \times K[X]/\mathcal{G}_\beta$ は群同型写像か?

U が準同型写像であるとは, 以下の 3 つの条件が成り立つときにいう. これらを順番に検証していく.

(i) $^\forall a, b \in K[X], f(a+b) = f(a) + f(b)$

(ii) $^\forall a, b \in K[X], f(ab) = f(a)f(b)$

(iii) $f(1_{K[X]}) = 1_{K[X]/\mathcal{G}_\alpha \times K[X]/\mathcal{G}_\beta}$ （$1_{K[X]}$ は $K[X]$ の単位元, $1_{K[X]/\mathcal{G}_\alpha \times K[X]/\mathcal{G}_\beta}$ は $K[X]/\mathcal{G}_\alpha \times K[X]/\mathcal{G}_\beta$ の単位元である. ）

- (i) について
  $f, h \in K[X]$ とする.

$$\begin{aligned} U(f+h) &= ([f+h]_{\mathcal{G}_\alpha}, [f+h]_{\mathcal{G}_\beta}) \\ &= ([f]_{\mathcal{G}_\alpha} + [h]_{\mathcal{G}_\alpha}, [f]_{\mathcal{G}_\beta} + [h]_{\mathcal{G}_\beta}) \\ &= ([f]_{\mathcal{G}_\alpha}, [f]_{\mathcal{G}_\beta}) + ([h]_{\mathcal{G}_\alpha}, [h]_{\mathcal{G}_\beta}) \\ &= U(f) + U(h) \end{aligned}$$

  よって (i) は成り立つ. 同じようにして (ii) も成り立つ.
- (iii) について
  $K[X]$ の単位元は 1, $K[X]/\mathcal{G}_\alpha \times K[X]/\mathcal{G}_\beta$ の単位元は $([1]_{\mathcal{G}_\alpha}, [1]_{\mathcal{G}_\beta})$ である. よって, $U(1) = ([1]_{\mathcal{G}_\alpha}, [1]_{\mathcal{G}_\beta})$ となるので成り立つ.

以上より写像 U は準同型写像であることが分かった. よってこの写像に準同型定理を適応することができる. つまり, 以下の写像 U' は同型写像である.

$$U' : K[X]/\mathrm{Ker}(U) \to \mathrm{Im}(U) \quad , \quad a + \mathrm{Ker}(U) \mapsto U(x)$$

さて, $\mathrm{Im}(U)$, $\mathrm{Ker}(U)$ を求めよう.

- $\mathrm{Ker}(U)$ について

$$\begin{aligned} f \in \mathrm{Ker}(U) &\Leftrightarrow {}^\exists f \in K[X] \ s.t. \ U(f) = 0_{K[X]/\mathcal{G}_\alpha \times K[X]/\mathcal{G}_\beta} \\ &\Leftrightarrow U(f) = ([0]_{\mathcal{G}_\alpha}, [0]_{\mathcal{G}_\beta}) \\ &\Leftrightarrow f = f_1 g_{1\alpha} + f_2 g_{2\alpha} + \cdots + f_s g_{s\alpha} \\ &\qquad = f_1 g_{1\beta} + f_2 g_{2\beta} + \cdots + f_t g_{t\beta} \\ &\Leftrightarrow f \in \langle \mathcal{G}_\alpha \rangle \times \langle \mathcal{G}_\beta \rangle \end{aligned}$$

  よって $\mathrm{Ker}(U) = \langle \mathcal{G}_\alpha \rangle \times \langle \mathcal{G}_\beta \rangle$
- $\mathrm{Im}(U)$ について
  写像 U の値域である $K[X]/\mathcal{G}_\alpha \times K[X]/\mathcal{G}_\beta$ の濃度と $K[X]/\mathrm{Ker}(U)$ の濃度が同じであればよい. ここで重要になるのが, 一般的なグレブナー基底 $\mathcal{G}$ に対し, $K[X]/\mathcal{G}$ の濃度はどのように決定されるのかである. 思うに, これは $\mathcal{G}$ が具体的に求まらなければ分からないはずだ. よってこれ以上のことは今の条件では分からない.

結果として, $K[X]/\langle \mathcal{G}_\alpha \rangle \times \langle \mathcal{G}_\beta \rangle \cong K[X]\mathcal{G}_\alpha \times K[X]/\mathcal{G}_\beta$ のようなものが成り立つことは証明できなっかった.

5 おわりに

今回の研究は, 授業で習った環の事柄を多項式環にあてはめたような内容となった. 授業では例として整数環を扱ったが, 多項式環との違いがやはりみられる. それは, 多項式環の剰余環は無数にあるので, 条件を適切に設けないと欲しい結果が得られないということである. 条件の見直しと, ところどころ論理的におかしい議論を進めていたのでそこの訂正を行っていきたい.

途中から気になったこととして, グレブナー基底を導入せずとも, 多項式環 $K[X]$ のイデアル I のみで剰余環 $K[X]/I$ を考えることができたのではないかということである. 私は, 多項式を割ったときの「余り」に焦点を当てて, 余りが一致するという性質を持つグレブナー基底を使うことにしたが, 自然な流れとしてはイデアル I のみを用いて考えるべきであろう. つまり, 今までの議論はグレブナー基底を使わなくとも進めることができたかもしれない. 次回以降に, イデアルから考えてみて, グレブナー基底が必要かどうか研究してみたい.