NOTE BOOK
CONTAINING BEST RULED FOOLSCAP

代数学 II

No. 27

洛北

猪瀬博司

コクヨ
意匠登録 No.151492

§23 因数分解

◦ 因数分解の基本定理

因数分解の基本定理

Sが単位要素をもつ整域で，素因子分解の一意性が成り立つとすると，多項式環 $S[x]$ にも素因子分解の一意性が成り立つ。

（この定理の証明に以下2つの補題を証明する）

◦ 原始多項式

原始多項式

$f(x)=\sum_{i=0}^{n} a_i x^i$ を0と異なる $S[x]$ の多項式とする。$f(x)$ の係数 $a_0, \cdots, a_n$ の Sにおける最大公約元（§19の意味での）を d とする。d をくくり出すと

$$f(x)=d\,g(x)$$

となり $g(x)$ の係数の最大公約元は1である。$g(x)$ と d は単元因子を除いて一意的にきまる。この $g(x)$ のように係数の最大公約元が1の時この多項式をSにおける原始多項式という。

◦ 補題1　2つの原始多項式の積は，原始多項式である。

［証明］　原始多項式 $f(x)$, $g(x)$ の積が公約元 d をもつとす。d の素因子の1つを p とすると $f(x)$, $g(x)$ は公約元に1（又は単元）しかもたないから $f(x)$, $g(x)$ の係数の中にはどちらも p で割りきれないものが1つはある。その1番次数の低い係数の項を $a_\lambda x^\lambda$, $b_\mu x^\mu$ とする。すると $f(x)g(x)$ の $x^{\lambda+\mu}$ の項は　$a_\lambda b_\mu + a_{\lambda+1} b_{\mu-1} + a_{\lambda+2} b_{\mu-2} + \cdots + a_{\lambda-1} b_{\mu+1} + \cdots$

となるがこの初項以下はいずれも p の倍元となり，初項だけが p の倍元とならないから $x^{\lambda+\mu}$ の係数は p の倍元とならず仮定に反す。

◦ Sの商体を Z とする $Z[x]$ の中では多項式 $\varphi(x)$ は既約多項式の積に一意的に分解される。（§19による）　$Z[x]$ の多項式は

$$\varphi(x)=\frac{F(x)}{b} \qquad (b\in S,\ F(x)\in S[x])$$

と表わされる。$F(x)$ は原始多項式 $f(x)$ と d との積になるから

$$\varphi(x)=\frac{a}{b}f(x) \qquad (a, b\in S,\ f(x)\in S[x] \text{ で原始多項式})$$

この対応は単元の違いを除けば一意的である。（証明省略）

注）　$Z[x]$ の単元はSの要素全体になる。

○ 補題 2　前ページのような対応で $Z[x]$ 内の多項式は $S[x]$ の原始多項式の積に，又逆に原始多項式の積は $Z[x]$ 内の多項式に対応される。$\varphi(x)$ が $Z[x]$ で既約ならば，$f(x)$ も又 $S[x]$ で既約である。又逆に $f(x)$ が $S[x]$ で既約ならば，$\varphi(x)$ も又 $Z[x]$ で既約である。

［証明］ 2つの多項式

$$\varphi(x) = \frac{a}{b} f(x) \quad , \quad \psi(x) = \frac{c}{d} g(x)$$

に対して

$$\varphi(x)\psi(x) = \frac{ac}{bd} f(x) g(x)$$

だから　$\varphi(x)\psi(x)$ に対しては補題1より $f(x)g(x)$ が対応する。
逆に $f(x)g(x)$ に対して $\varphi(x)$，$\psi(x)$ を a, b, c, d を適当にとると積 $f(x)g(x)$ に対して $\varphi(x)\psi(x)$ が対応するが a, b, c, d の値は単元違いになるだけである。$\varphi(x)$ が $Z[x]$ で既約でそれに対応する原始多項式が積 $f(x)g(x)$ になったとすると上述からすぐに $\varphi(x)$ が分解されてしまい仮定に反する。逆も同様。

○ 基本定理の証明
補題2によって $Z[x]$ の素因子分解が $S[x]$ の素因子分解に単元の違いを除いて一意的に対応せられる。よって $S[x]$ の原始多項式には素因子分解の一意性が成り立つ。次に $S[x]$ の任意の多項式をとる。これのある素因子分解が

$$g(x) = a_1 \cdots a_s \, g_1 g_2 \cdots g_r \quad (a_i \in S,\ g_i \in S[x])$$

となったとする。この時 g_i は原始多項式である。(∵ 原始多項式でなければ $d g_i'$ の形に分解される。）従って積 $g'(x) = g_1 \cdots g_r$ は原始多項式である。$a_1 \cdots a_s = d$ とすれば $g(x) = d\, g'(x)$; $g'(x)$ は原始多項式となる。従って $g(x)$ の任意の分解はそれを $d \times$ 原始多項式の積になおしてからそれぞれ素因子分解している。d も $g'(x)$ も素因子分解の一意性が成り立つから $g(x)$ も素因子分解の一意性が成り立つ。
よって $S[x]$ に於ても定理が証明された。

○ $S[x]$ 上の多項式 $f(x)$ が $Z[x]$ 上で可約なら，実は $S[x]$ 上で可約である。

［証明］ $F(x)$ $(\in S[x])$ を $d \times f(x)$，(原始多項式）の形に直す。$F(x)$ が $Z[x]$ で可約なのだから $F[x] \in Z[x]$ とみて，補題2を適応すると $F(x)$ の分解には $f(x)$ の $S[x]$ での分解が対応

するから 結局 $F(x)$ は $S[x]$ でも可約となる。

- 上の定理をいいかえると $F(x)$ が $S[x]$ で既約なら，$\Sigma[x]$ でも既約である。
- これらの定理の逆も又成り立つ。

	$S[x]$		$\Sigma[x]$
$f(x) \in S[x]$	既約	$\longleftrightarrow$	既約
$f(x) \in S[x]$	可約	$\longleftrightarrow$	可約

（即ち既約，可約は $S[x]$ で考えても $\Sigma[x]$ で考えても変わらない。）

- 基本定理から帰納法によって次の定理が導ける。
  S が単位要素をもつ整域で，素因子分解の一意性が成り立てば多項式環 $S[x_1, x_2, \cdots, x_m]$ に於ても一意性が成り立つ。

原始的 ◦ $x_1, \cdots, x_{m-1}$ に対して原始的 多項式環 $K[x_1, \cdots, x_m]$ の要素 f が $x_1, \cdots, x_{m-1}$ のみに関係する因子をもたない時，（但し K は体とする）

Sm. 1. ◦ $S[x]$ の単元は，S の単元である。

［証明］ $S[x]$ の単位要素は 1 であるから $S[x]$ の単元の1つを f とすれば $1 = f \cdot f^{-1}$，f の素因子を p とせば 1 はその素因子の中に p を含まなければならないが 1 は 1 としか分解できないから p は 1 に S の単元を乗じた数即ち S の単元自身に等しくなる。f は単元の積だからもちろん S の単元となる。

Sm 2 ◦ 同次多項式を因数分解しても，因数としては同次多項式しかあらわれない。

［証明］ $S[x_1, \cdots x_m]$ の任意の同次多項式を f としその因数分解を

$$f = a\,p_1 p_2 \cdots p_r \qquad (a \in S,\ p_i \in S[x_1, \cdots, x_m])$$

この式の両辺に $x_1, x_2, \cdots, x_m$ の代わりに $x_1 t, x_2 t, \cdots, x_m t$ を入れる。すると

$$f' = a\,p_1' p_2' \cdots p_r'$$

となる。ところが §20 より $f' = t^m f$ であるからこれを代入すると

$$p_1' p_2' \cdots p_r' = t^m\, p_1 p_2 \cdots p_r$$

p_i は素元だから $p_1', \cdots, p_r'$ のうちに $p_\alpha' = t^s p_i g$ なる p_α' が存在する。（これは t に関係せず f を定めた時にきまる）

両辺に $t=1$ を代入すると

$$P_j = P_i g|_1 g$$

ところが P_j は $S[x_1, \cdots, x_n]$ で既約（素元）だから g は単元となり実は P_j と P_i は全く同じ因子となる。もとの式にこれを代入すると

$$P_i' = t^s P_i$$

即ち P_i は同次多項式である。

$S_m 3$ ◦ 行列式

$$\Delta = \begin{vmatrix} x_{11} & \cdots & x_{1n} \\ \cdots & & \cdots \\ x_{n1} & & x_{nn} \end{vmatrix}$$

は多項式環 $S[x_{11}, \cdots, x_{nn}]$ で既約である。

［証明］ まずこの命題は $n=1$ に於てはなりたつ。今 $n=m-1$ で成り立つと仮定する。Δ は $x_{11}, \cdots, x_{1m}$ の1次式であるからもし因数分解 fg ができたとすると どちらか一方に $x_{11}, \cdots, x_{1m}$ がすべて含まれる。更にそれは1次式であるそれを $f = a_{11}x_{11} + \cdots + a_{1m}x_{1m}$ とすれば

$$\Delta = (a_{11}x_{11} + \cdots + a_{1m}x_{1m})\, g$$

の形に成りえる。よって $\Delta = D_{11}x_{11} + \cdots + D_{1m}x_{1m}$ であるから $D_{11} = a_{11}g$ となり $m-1$ 次の行列式は既約だから g が単元か a_{11} が単元かであるが g が単元だと Δ は既約となって定理が成り立つ。もし a_{11} が単元だとこのような分解はすべての行に関していえるから

$$\Delta = \sum_{h=1}^{m}{}' (a_{h1}x_{h1} + \cdots + a_{hm}x_{hm})$$

となる。ところが同様なことが列についてもいえ

$$\Delta = \sum_{j=1}^{m} (b_{1j}x_{1j} + \cdots + b_{mj}x_{mj})$$

となる。1次式 $c_1x_1 + \cdots + c_m x_m$ (c_i は単数）は既約だから両方の m 個の因子が一致しなければならず このようなことはおこらない。

$S_m 4$ ◦ 有理整係数の多項式が一次因数をもつ判定条件

［解答］ 多項式を $f(x) = a_n x_n + \cdots + a_0$ とする

$f(x) = (cx+d)\, g(x)$ ならば $c \mid a_n$、$d \mid a_0$ だから a_n, a_0 の約数の組み合わせ $\frac{d}{c}$ を f に代入して 0 になればよい。

Sn.5 ◦ 多項式 x^4-x^2+1 は，xを不定元とする整係数多項式環 $Z[x]$ において既約である。この多項式はガウスの整数環で可約である。

[証明] もし x^4-x^2+1 は $Z[x]$ に於て1次因数をもたない。実際 $f(\pm 1)=1$ (Sn4) である。従って $f(x)=x^4-x^2+1$ が可約なら $f(x)=(x^2+ax+b)(x^2+cx+d)$ の形になる。$bd=1$ だから $b=d=1$ か $b=d=-1$ である。三次の項は0だから $a=-c$，同様に $ac=1,-3$ ，$a^2=-1,3$ このような整数は存在ない。(よって $f(x)$は有理係数多項式 $P[x]$ でも既約)

又ガウスの整数環 $Z[i]$ では実際に

$$x^4-x^2+1=(x^2+ix+1)(x^2-ix-1)$$

となるから可約である。

§ 24 既約性の判定

◦ Sは単位要素をもつ整域で，素因子分解の一意性が成り立つとする。

D アイゼンシュタインの定理

アイゼンシュタインの定理

Sの素元Pで $a_m \not\equiv 0\ (P)$，$a_i \equiv 0\ (P)$，$a_0 \not\equiv 0\ (P^2)$，$(i<m)$ を満たすものが存在すれば，$f(x)$は $S[x]$ で定数因子を除き既約である。

[証明] $f(x)=g(x)\,h(x)$ とする。(分解できたと仮定) $g(x)$と$h(x)$の次数 r,s はどちらも正で $r+s=m$ ($\deg f$) である。$g(x)$の末項 b_0 と $h(x)$の末項 c_0 の積は Pで割りきれ P^2 で割りきれない 従ってどちらか一方のみがPで割りきれる 例えばその方を $g(x)$ とする。すると $h(x)$の係数はすべてPの倍元にはならないから $h(x)$ のPの倍元でない最低次の項を $c_\lambda x^\lambda$ $(\lambda \geqq 1)$ とする 更に g,h の x^kの係数をそれぞれ b_k, c_k で表わすと $f(x)$ の x^λの項の係数は

$$a_\lambda = c_\lambda b_0 + c_{\lambda-1}b_1 + \cdots + c_0 b_\lambda$$

となり第1項以下は皆 Pで割りきれるから a_λはPで割りきれない。$m>\lambda\geqq 1$ だから a_λ はPで割きれなくてはならず仮定に反す。

Sn.1 ◦ $P_1,\cdots,P_r$ を異なった素数とし，$m>1$ とすると $\sqrt[m]{P_1P_2\cdots P_r}$ は無理数である

[証明] 方程式 $x^m-P_1P_2\cdots P_r=0$ が既約なことを証明すればよい。

先のアイゼンシュタインの定理に於て Pを任意の P_i とおけばよい。

Sn.2 ◦ 多項式 x^2+y^2-1 は $P[x,y]$ で既約である。但しPは $+1 \neq -1$

とする。

［証明］ 環を $P[y]$ とし 多項式 x^2+y^2-1 を $P[y]$ 上の多項式と考える。 $y^2-1=(y+1)(y-1)$ （但し $\pm 1 \in P$ と考えている） $1 \neq -1$ だから $y+1 \neq a(y-1)$ $(a \in P)$ ∵ $y=1$ を代入してみればわかる。よって $y+1$ は $P[y]$ の素元である。から x^2+y^2-1 にアイゼンシュタインの定理を使うと x^2+y^2-1 が既約であることがわかる。

Sm. 3 ○ 整係数多項式環 $Z[x]$ において，多項式

$$x^4+1 \quad , \quad x^6+x^3+1$$

は既約である。

［証明］ x^4+1 が可約であれば $(x+1)^4+1$ は可約である。
$(x+1)^4+1 = x^4+4x^3+6x^2+4x+2$ であるから $p=2$ として，アイゼンシュタインの定理を使うと，これが既約なことがわかる。よって x^4+1 も既約である。
後の式も同様にして $x^6+6x^5+15x^4+21x^3+18x^2+9x+3$ となり $p=3$ として定理が使え x^6+x^3+1 が既約となる。

○ 剰余類による既約性の判定

アイゼンシュタインの定理は $f(x)=g(x)h(x)$ を p^2 を法とした剰余類に導きこれから不合理を出して証明される。このような考えを他の場合にも応用する。いくつかの方法を示す。

1. $f(x)$ が環 S の1つの要素 q を法とした合同式に変えて，もしそれが q を法として因数分解されない（既約）なら S 上でも既約である。
この際 S が有理整数環 Z なら q を法とする剰余環 $Z/(q)$ には与えられた次数の多項式が有限個しかないから有限個の可能性をためすだけでよい。
2. $f(x)$ が有理整数環 Z の多項式で素数を法とする剰余体 $Z/(q)$ で因数分解されればそこでは因数分解の一意性が成り立つから，因子 $g(x)$ と $h(x)$ の次数や q を法とした時の式の形等に条件を加えることができる。

○ アイゼンシュタインの定理の拡張

P を S の素元とする。$(c,p)=1$ として $f(x)$ の各項 $ax^\lambda = cp^\mu x^\lambda$ に，指数の組 (λ,μ) を対応さす。各項 $cp^\mu x^\lambda$ に重み $\alpha\lambda+\beta\mu$ をつける。

重み 但し $(\alpha,\beta)=1$ で $\beta>0$ とする。この時 $f(x)$ に項の重みの最小値が2項あらわれるようにする。$\alpha\lambda+\beta\mu$ の最小値を γ にする。(λ,μ) の2つの値の組を，例えば (λ_1,μ_1)，(λ_2,μ_2) とし λ_i はできるだけ小さく，

λ_2はできるだけ大きくとる。

$$\alpha\lambda_1+\beta\mu_1=\alpha\lambda_2+\beta\mu_2=\gamma$$

から　$\alpha(\lambda_2-\lambda_1)+\beta(\mu_2-\mu_1)=0$

となるから，$\lambda_2-\lambda_1$はβで割りきれる。

$$\lambda_2-\lambda_1=m\beta,\ \mu_2-\mu_1=-m\alpha,\quad m=(\lambda_2-\lambda_1,\mu_2-\mu_1)$$

となるこの時次の定理が成り立つ．

▷ $f(x)$が2つの多項式に分解されるならば，2つの因数の次数は，必ず

$$m_1\beta+\gamma_1,\qquad m_2\beta+\gamma_2 \qquad (1)$$

$$(m_1,m_2,\gamma_1,\gamma_2\geqq 0,\quad m_1+m_2=m,\quad \gamma_1+\gamma_2=n-m\beta)$$

の形をしている。

［証明］　$f(x)=g_1(x)g_2(x)$とし$g_1(x)$の項の最小の重みをγ_1 $g_2(x)$の項の最小の重みをγ_2とする。$g_1(x)$の重みγ_1の項のうち最低次δのものをdx^δとし最高次εのものをex^εとする，同様に$g_2(x)$の重みγ_2の項のうち最低次のものをrx^ρ，最高次のものをsx^σとする。積$f(x)=g_1(x)g_2(x)$の重み$\gamma_1+\gamma_2=\gamma$の項のうち$drx^{\delta+\rho}$が最低次で$esx^{\varepsilon+\sigma}$が最高次である。よってこれを前の記号とあわせて

$$\gamma_1+\gamma_2=\gamma,\quad \delta+\rho=\lambda,\quad \varepsilon+\sigma=\lambda_2$$

でなければならない。故に　$(\varepsilon-\delta)+(\sigma-\rho)=\lambda_2-\lambda_1=m\beta$

となる。ところが　$\varepsilon-\delta$，$\sigma-\rho$も又βで割りきれるから

$$\varepsilon-\delta=m_1\beta,\quad \sigma-\rho=m_2\beta\quad とにて\quad m_1+m_2=m$$

である．$g_1(x)$の次数は少なくてもεであるから$\geqq m_1\beta$で，同様に$g_2(x)$の次数は少なくても$m_2\beta$である。よって定理が成り立つ。

◦系1　2つの次数(1)のうち少なくても一方は，$\geqq\beta$である。

◦系2　$f(x)$の最初の項と最後の項が最小の重みγをもつ時は，g_1，とg_2の次数はβで割りきれる。

◦系3　$\beta=n$ならば　$f(x)$は既約である（系1より）

注）特に$\alpha=1$，$\beta=\gamma=n$とするとアイゼンシュタインの定理が得られる。

§25　有限回の手続きで因数に分解する方法

▷ Sではすべての要素が有限回の手続きで素因子に分解され，更にSには有限個の単元しかないとすると．S[x]のすべての多項式が有限回の手続きで素因

子に分解できる。次にこの方法を説明する。

○ $f(x)$ を $S[x]$ における n 次の多項式とする。$f(x)$ が可約ならば，その因数の1つは次数が $\leqq \frac{n}{2}$ である。$f(x)$ の次数 $\leqq \frac{n}{2}$ の因数 $g(x)$ がわかればよい。$s+1$ 個のかってな S の要素 $a_0, a_1, \cdots, a_s$ に対する函数の値 $f(a_0), f(a_1), \cdots, f(a_s)$ を計算する。$g(x)$ が $f(x)$ の因数なら $g(a_0)$, $g(a_1), \cdots, g(a_s)$ は $f(a_0), \cdots, f(a_s)$ の因数となる。$f(a_i)$ は S で有限個の約元しかもたないから各 $g(a_i)$ には有限個の可能性があるにすぎない。それらは仮定により S 内ですべて見つけられる。これらの値の可能な組み合わせ $g(a_0), \cdots, g(a_s)$ をかってに作ると §22 の定理より，$g(x)$ がただ1つ定まる。この求まった各々の $g(x)$ について $f(x)$ を割りきるかどうか調べればよい。このようにして $g(x)$ が定まらない（どれも $f(x)$ を割りきらない）なら $f(x)$ は既約である。又 $g(x)$ が少なくても1つみつければ又それぞれにつき同様のことをくり返すと最後に $f(x)$ の因数分解が得られる。

○ 上の定理から帰納法によって $S[x_1, \cdots, x_m]$ の因数分解を有限回の手続きで求めることができる。

Sm. 1. ○ $Z[x]$ において

$$f(x) = x^5 + x^4 + x^2 + x + 2$$

を因数分解する。

[解答] $f(x)$ に1次の因数があれば $f(\pm 1)$, $f(\pm 2)$ のどれかが 0 になるがどれも 0 とならないので1次因数はない。

$f(x)$ は可約なら2次の因数をもつからそれを x^2+ax+b と書く。

ここで b は ± 1, ± 2 のいずれかである。よって因数の可能性として

x^2+ax+1, x^2+ax-1, x^2+ax+2, x^2+ax-2

が考えられる。$f(0)=2$, $f(-1)=2$ だからこれを各々に代入すると

x^2+ax+1 から　$2-a=1$, $2-a=-1$, $2-a=2$, $2-a=-2$

より　$a=1, 3, 2, 4$ がでてくる。$a=1$ とすると

$x^5+x^4+x^2+x+2 = (x^2+x+1)(x^3-x+2)$ となってうまく分解される。

Sm. 2 ○ $Z[x, y, z]$ において

$$f(x, y, z) = -x^3 - y^3 - z^3 + x^2(y+z) + y^2(x+z) + z^2(x+y) - 2xyz$$

を分解せよ。

[解答] $f(x, y, z)$ は3次の同次式であるからもし可約なら1次の

第4章 §25 ~ §26

同次式 $ax+by+cz$ を含むはずである。x^3, y^3, z^3 のそれぞれの係数は -1 であるから $|a|=|b|=|c|=1$ である。そのうち $a=1$ とする。(単元の違いは無視) すると式の可能性として

$x+y+z$, $x+y-z$, $x-y+z$, $x-y-z$

が残る。それぞれで $f(x,y,z)$ を割ると結局次の式が得られる

$$f(x,y,z)=(x+y-z)(y+z-x)(z+x-y)$$

§26 対称函数

対称函数

▷ Rを単位要素有する可換環とする。

$R[x_1,x_2,\cdots,x_n]$ の多項式が、不定元 $x_1,\cdots,x_n$ にどんな置換をほどこしても変わらない時 この多項式を 変数 $x_1,\cdots,x_n$ の(有理整)対称函数という。

基本対称函数 ◦ 新しい不定元 z をとり $f(z)=(z-x_1)\cdots(z-x_n)=z^n-\sigma_1 z^{n-1}+\cdots+(-1)^n\sigma_n$ とおく。この時係数 $\sigma_1,\sigma_2,\cdots,\sigma_n$ は $x_1,\cdots,x_n$ の対称函数である。この対称函数を $x_1,\cdots,x_n$ の基本対称函数という。

注)
$$\begin{cases}\sigma_1=x_1+\cdots+x_n\\ \sigma_2=x_1x_2+\cdots+x_{n-1}x_n\\ \cdots\cdots\\ \sigma_n=x_1x_2\cdots x_n\end{cases}$$

重み ◦ 単項式 $c\sigma_1^{\mu_1}\sigma_2^{\mu_2}\cdots\sigma_n^{\mu_n}$ の重み (但し $c\in R$)

$$\mu_1+2\mu_2+\cdots+n\mu_n$$

◦ 多項式 $\sum c\sigma_1^{\mu_1}\cdots\sigma_n^{\mu_n}$ の重み

多項式の各項の重み(上の意味)のうち最大のもの。

注) 重みの定義から $c\sigma_1^{\mu_1}\cdots\sigma_n^{\mu_n}$ の x_i の次数とその重みは一致する。($\because$ σ_j の x_i に対する次数は j である) 従って重み k の多項式 $\varphi(\sigma_1,\sigma_2,\cdots,\sigma_n)$ の x_i に対する次数は k 以下である。

対称函数の基本定理 ▷ $R[x_1,\cdots,x_n]$ の次数 k の有理整対称函数は、基本対称函数の重み k の多項式 $\varphi(\sigma_1,\cdots,\sigma_n)$ の形に一意的にあらわすことができる。

[証明] $n=1$ の時定理は成りたつ 次に $n-1$ 個の変数の時定理が成りたつと仮定する。0次の n 変数多項式に対しては定理は成り立つ。次数 $<k$ の多項式に対して定理が成り立つと仮定する。(2重に数学的帰納法を使う)
今 $R[x_1,\cdots,x_n]$ の対称式 $f(x_1,x_2,\cdots,x_n)$ を k 次の対称式と

する。f で $x_m=0$ とした函数 $f(x_1,\cdots,0)$ を考えると、これは $R[x_1,\cdots,x_{m-1}]$ の対称函数だから仮定より

$$f(x_1,\cdots,0)=\varphi(\sigma_1',\sigma_2',\cdots,\sigma_m')$$

となる。但し σ_i' というのは $n-1$ 個の変数の基本対称式である。この σ_i' は σ_i（n 個の変数の基本対称式）で $x_m=0$ とおいて求められる。先の $f(z)$ で $x_m=0$ とすれば $f(z)_0=z^m-\sigma_1' z^{m-1}+\cdots+(-1)^n\sigma_m'$ なる式が導ける。ここで表われた σ_i' の函数 φ は $x_1,\cdots,x_{m-1}$ に関して重み $\leqq k$ をもつ。よってこれから n 個の変数の函数 $\varphi(\sigma_1,\cdots,\sigma_m)$ の $x_1,\cdots,x_m$ に関する重みも k 以下となる。

多項式
$$f_1=f(x_1,\cdots,x_m)-\varphi(\sigma_1,\cdots,\sigma_m)$$

をとると、これは重み $\leqq k$ をもつ（$\because$ f,φ の重み（x に関する次数）は k 以下）更に f_1 は対称式である。ところが f_1 に $x_m=0$ を代入すると $f_1=0$ となるから f_1 は x_m を因数にもつ，f_1 が対称式であることからすべての x_i を因数として f_1 はもつ。故に

$$f_1=\sigma_m\, g(x_1,\cdots,x_m)\quad ,(g \text{ は対称式})$$

ここで g は 次数 $\leqq k-n<k$ をもつ よって帰納法の仮定より

$$g(x_1,\cdots,x_m)=\psi(\sigma_1,\cdots,\sigma_m)$$

となる。故に

（下式の重みは k となる）
$$f(x_1,\cdots,x_m)=f_1+\varphi=\sigma_m\psi(\sigma_1,\cdots,\sigma_m)+\varphi(x_1,\cdots,x_m)$$

即ち f は確かに帰納法から基本対称函数の函数として表わせる。次にこの f が一意的に基本対称函数によって表わせることを証明する。

$\varphi_1(y_1,\cdots,y_m)\neq\varphi_2(y_1,\cdots,y_m)$ ならば

の時 $\varphi_1(\sigma_1,\cdots,\sigma_m)\neq\varphi_2(\sigma_1,\cdots,\sigma_m)$

を証明すればよい。$n=1$ の時は成り立つ。次に変数の個数 $<n$ に対しては定理は成り立つと仮定する。但し定理のいう式を移項して

$$\varphi(y_1,\cdots,y_m)\neq 0 \quad \text{ならば}\quad \varphi(\sigma_1,\cdots,\sigma_m)\neq 0$$

を証明する。仮にこの定理を満たさない函数があったとし、そのうち y_m において最低次のものを $R[y_1,\cdots,y_{m-1}]$ 上の y_m の多項式とみと y_m の冪乗別に整理する。 $\varphi_m y_m^m+\cdots+\varphi_0\neq 0$

第4章 §26

σ_i の方も σ_m の累乗別に整理する。

$$\varphi_m(\sigma_1, \cdots, \sigma_{n-1})\sigma_m^m + \cdots + \varphi_0(\sigma_1, \cdots, \sigma_{n-1}) = 0$$

この時 φ_0（即ち $\varphi_0(y_1, \cdots, y_{m-1})$）は 0 ではない。なぜなら
もし φ_0 が 0 だと $\varphi(y_1, \cdots, y_m)$ は y_m で割りきれることになり
m次以下（y_m について）の多項式で定理を満たさぬものが存在する。
（φ は y_m について最低次の定理を満たさぬ式と定義している。）
よって $\varphi_0 \neq 0$ しかし σ_i の式の方は $x_m = 0$ とおくと

$$\varphi_0(\sigma_1', \cdots, \sigma_{m-1}') = 0, \quad \varphi_0(y_1, \cdots, y_{n-1}) \neq 0$$

となり $n-1$ 個の変数については定理は成り立つから このようなことは
仮定に反し 結局すべての自然数 n について定理は成り立つ。

注） 対称式の間に有理整式が成り立つ時 x_i が R の要素 にならなくても
式はそのままなり立つ。x_i が $R[z]$ で1次因数に完全に分解され
る多項式 $f(z)$ の根であれば $f(z)$ の根の対称式は $f(z)$ の係数の
有理整式で表わされる。

▷ 計算法

◦ 与えられた多項式を辞書式に整頓する。その最初の項 $ax_1^{\alpha_1} \cdots x_m^{\alpha_m}$ と同じ初項をもつ対称式 $a\sigma_1^{\alpha_1-\alpha_2}\sigma_2^{\alpha_2-\alpha_3} \cdots \sigma_m^{\alpha_m}$ の差をとる 残った式に対しても同様なことを続けると 最後に差が 0 となる。

Sm. 1 ◦ 上の（計算法の下の）定理の証明。

［証明］ 対称式を辞書式に整頓する（$\alpha_1-\beta_1, \alpha_2-\beta_2, \cdots, \alpha_m-\beta_m$ の最初に表われる 0 でない項が正の時 $ax_1^{\alpha_1} \cdots x_m^{\alpha_m}$ を $bx_1^{\beta_1} \cdots x_m^{\beta_m}$ より先に書く仕方）この時の初項を $ax_1^{\alpha_1} \cdots x_m^{\alpha_m}$ とする。上述の差によって 対称式 $\varphi(x_1, \cdots, x_m)$ の方は一番前の項（初項）がなくなり 同様に $a\sigma_1^{\alpha_1-\alpha_2} \cdots \sigma_m^{\alpha_m}$ もこれを $x_1, \cdots, x_m$ の式に直した時の 初項がなくなる。他の項はみな $ax_1^{\alpha_1} \cdots x_m^{\alpha_m}$ より後にくるのだから 差 $\varphi - a\sigma_1^{\alpha_1-\alpha_2} \cdots \sigma_m^{\alpha_m}$ の初項は当然 $ax_1^{\alpha_1} \cdots x_m^{\alpha_m}$ と比べた時その後に 置かれるべきである。これから一つの $ax_1^{\alpha_1} \cdots x_m^{\alpha_m}$ が与えられた時この後に 置かれるべき項が係数の違いを除いて有限個であることが 証明されればよい。
但し $\alpha_1 \geqq \alpha_2 \geqq \cdots \geqq \alpha_m$ は仮定しておく。（対称式であるから）
今 $ax_1^{\alpha_1} \cdots x_m^{\alpha_m}$ の後に続くべき 次々と差をとって得られる 多項式の初項に対しても $cx_1^{\gamma_1} \cdots x_m^{\gamma_m}$ に $\gamma_1 \geqq \gamma_2 \geqq \cdots \geqq \gamma_m$ は同様に成り立つ。ところが 明らかに $\gamma_1 \leqq \alpha_1$ であるから $\gamma_1, \cdots, \gamma_m$ の取りうる

可能性は制限を $\alpha_1 \geqq r_1, r_2, \cdots, r_m \geqq 0$ とゆるめて多くみつもっても $(\alpha_1+1)^n$ である。よって n, α_1 は有限の値であるから $\varphi(x)$ の後に続く差の多項式 $\varphi_1(x), \cdots, \varphi_m(x)$ も有限個続くにすぎず結局最後には差が0となる。

Sm. 2 ◦ 任意の n について累乗和

$$\Sigma x_i \;,\; \Sigma x_i^2 \;,\; \Sigma x_i^3$$

を基本対称式で表わす。

［解答］ Σx_i は σ_1 そのものである $\Sigma x_i = \sigma_1$

Σx_i^2 は辞書式に書きかえて σ_1^2 を引くと $-2\sigma_2$ になるから

$\Sigma x_i^2 = \sigma_1^2 - 2\sigma_2$. Σx_i^3 は前ページの計算法をつかって σ_1^3 を引くと

$$-6\Sigma x_i x_j x_k - 3\Sigma x_i^2 x_j$$

となるこれから $-3\sigma_1\sigma_2$ を引くと

($i \neq j, j \neq k, i \neq k$, $r \neq s$

$$\sigma_1\sigma_2 = \Sigma x_i \Sigma x_j x_k = \Sigma x_i x_j x_k = 3\Sigma x_i x_j x_k + \Sigma x_r^2 x_s$$

であるから その差は $-3\Sigma x_i x_j x_k$ ($i \neq j, k, j \neq k$)

となりそれは $-3\sigma_3$ になるから

$$\Sigma x_i^3 = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3$$

となる。

Sm. 3 ◦ $\Sigma x_i^p = s_p$ とおくと公式

$p \leqq n$ の時

$$s_p - s_{p-1}\sigma_1 + s_{p-2}\sigma_2 - \cdots + (-1)^p p\,\sigma_p = 0$$

$p > n$ の時

$$s_p - s_{p-1}\sigma_1 + \cdots + (-1)^n s_{p-n}\sigma_n = 0$$

が成り立つ。これを用いて累乗和 $s_1, s_2, \cdots, s_5$ を基本対称式で表わす。

［証明］ p, n に関する帰納法で証明する。まず $p=1$ の時は n の値に関係なく $\Sigma x_i = s_1 = \sigma_1$ であるから成り立つ よって $p < u$ に対して定理が成り立つとする。又 $n=1$ の時は σ の値に関係なく $\Sigma x_i^p = \sigma_1^p$ ととれるから $p = u$ に対して $n < m$ の時定理が成り立つと仮定する。

（もちろん $p < u$ の時はどんな n についても定理が成り立つと仮定している）

$n = m-1$ の時公式は成り立つから。m 個の変数の累乗和を s_p, $m-1$ 個の変数（不定元）の累乗和を s_p' . 同様に基本対称式を σ_i, σ_i' とすれば

$u \leqq m-1$ の時 $$s_u' - s_{u-1}'\sigma_1' + \cdots + (-1)^u u\,\sigma_u' = 0$$

第4章 §26

$u > m-1$ の時 $S'_u - S'_{u-1}\sigma'_1 + \cdots + (-1)^{m-1} S'_{u-m+1}\sigma'_{m-1} = 0$

ここで $S'_\alpha = S_\alpha - x_i^\alpha$ （iは任意）とできるから（

iにmを代表にとる。又 $\sigma'_r = \sigma_r - x_m \sigma'_{r-1}$ であるからこの2式を上式に代入すると

$u \leq m-1$ の時は各 $S'_{u-k}\sigma'_k$ が $S_{u-k}\sigma_k - S'_{u-k}\sigma'_{k-1}x_m + x_i^{u-k}\sigma_k$ となる。最後の項 $u\sigma'_u$ は $u\sigma_u - (u-1)\sigma'_{u-1} + \sigma'_{u-1}$ となる $u > m-1$ の方も最後の項を除いて同じことがいえる。

ところがこれらを別々にして加えると

$u \leq m-1$

$$(S_u - S_{u-1}\sigma_1 + \cdots + (-1)^u u\sigma_u) + x_m(S'_{u-1} - S'_{u-2}\sigma'_1 + \cdots + (-1)^{u-1}(u-1)\sigma'_{u-1})$$
$$+ (x_m^u - x_m^{u-1}\sigma_1 + \cdots + (-1)^{u-1}x_m\sigma_{u-1} + (-1)^u\sigma_u) = 0$$

となるこの第2項は $p = u-1,\ n = m-1$ とした時の定理の形だから仮定より0となる。この式はx_mの代わりに他のx_iでもよい。各x_iで作った上式をすべて加え合わせると

$$mA_1 - (S_u - S_{u-1}\sigma_1 + \cdots + (-1)^u u\sigma_u) = 0$$

となる即ち $(m-1)A_1 = 0$,（A_1は第1項を表わす）

$m > 1$ だから $A_1 = 0$ となる。

$u > m-1$ の時も同様なことを行なうと定理が成り立つことがわかる。

$S_0 = m$ と定義すれば定理の下の公式は実は上の公式と $p = m$ の点で一致する。σ_k $(k > m)$ に対して $\sigma_k = 0$ と定義すれば上の公式だけでたりる。

$S_1 \cdots\ S_1 - \sigma_1 = 0 \quad \therefore\ S_1 = \sigma_1$

$S_2 \cdots\ S_2 - S_1\sigma_1 + 2\sigma_2 = 0 \quad \therefore\ S_2 = \sigma_1^2 - 2\sigma_2$

$S_3 \cdots\ S_3 - S_2\sigma_1 + S_1\sigma_2 - 3\sigma_3 = 0 \quad \therefore\ S_3 = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3$

$S_4 \cdots\ S_4 - S_3\sigma_1 + S_2\sigma_2 - S_1\sigma_3 + 4\sigma_4 = 0$

$\therefore\ S_4 = \sigma_1^4 - 4\sigma_1^2\sigma_2 + 4\sigma_1\sigma_3 + 2\sigma_2^2 - 4\sigma_4$

$S_5 \cdots\ S_5 - S_4\sigma_1 + S_3\sigma_2 - S_2\sigma_3 + S_1\sigma_4 - 5\sigma_5 = 0$

$S_5 = \sigma_1^5 - 5\sigma_1^3\sigma_2 + 5\sigma_1^2\sigma_3 + 5\sigma_2^2\sigma_1 - 5\sigma_1\sigma_4 - 5\sigma_2\sigma_3 + 5\sigma_5$

Sm. 4 ○ S_pは前の意味とし Σは $\lambda_1 + \cdots + n\lambda_n = p$ を満たすすべてにわたるものとする時

$$S_p = \Sigma\, a_{\lambda_1,\cdots,\lambda_m}\sigma_1^{\lambda_1}\sigma_2^{\lambda_2}\cdots\sigma_m^{\lambda_m}$$

とおくと （同次の多項式は同じ重さの各項からなる基本対称式で表わせる（証明略））Sm. 3 より次の式を得る

$$a_{\lambda_1,\lambda_2,\cdots,\lambda_n} = a_{\lambda_1-1,\lambda_2,\cdots,\lambda_n} + a_{\lambda_1,\lambda_2-1,\cdots,\lambda_n} + \cdots + [+ (-1)^{\rho-1}\rho]$$

但し[ ]内は $\lambda_\rho=1$ で他のすべての $\lambda_i=0$ の時に表われる。
負の添数をもつすべての a は0とおく。
この帰納的関係により定まる $a_{\lambda_1,\cdots,\lambda_n}$ は

$$a_{\lambda_1,\cdots,\lambda_n} = \frac{(-1)^{\lambda_2+\cdots+\lambda_r} \cdot \rho(\lambda_1+\cdots+\lambda_n-1)!}{\lambda_1!\,\lambda_2!\cdots\lambda_n!}$$

である。　（r は n 以下の最大の偶数）

[証明]　公式は $\lambda_1+\cdots+\lambda_n=k$ を $\lambda_1'+\cdots+\lambda_n'=k-1$ の和に直す帰納的関係とみなされるから任意の $\lambda_1+\cdots+\lambda_n=k$ は $\bar\lambda_1+\cdots+\bar\lambda_n=1$ の和（正確には1次式）で表わされる。よって下の $a_{\lambda_1,\cdots,\lambda_n}$ が $\bar\lambda_1+\cdots+\bar\lambda_n=1$ の時条件を満たし，更に公式の示す帰納的関係を満たすことを証明すればよい。　まず $\lambda_1+\cdots+\lambda_n=1$ の時定理が成り立つことを示す。
この時 $\lambda_i \geqq 0$ ($i=1,\cdots,n$) であるから $\lambda_\rho=1$ で他の λ_i は皆0となる。
$a_{\lambda_1,\cdots,\lambda_n}$ の公式は

$$a_{\lambda_1,\cdots,\lambda_n} = (-1)^{\rho-1}\rho$$

となり条件を満たす。次に帰納的関係を証明する。（$\lambda_1+\cdots+\lambda_n \geqq 2$）

$$a_{\lambda_1-1,\lambda_2,\cdots,\lambda_n} = \frac{(-1)^{\lambda_2+\cdots}\ \lambda_1(\rho-1)(\lambda_1+\cdots+\lambda_n-2)!}{\lambda_1!\,\lambda_2!\cdots\lambda_n!}$$

- -

$$a_{\lambda_1,\cdots,\lambda_{2i},\cdots,\lambda_n} = \frac{(-1)^{\lambda_2+\cdots+\lambda_r-1}\ \lambda_{2i}(\rho-2i)(\lambda_1+\cdots+\lambda_n-2)!}{\lambda_1!\,\lambda_2!\cdots\lambda_n!}$$

$$a_{\lambda_1,\cdots,\lambda_{2i+1},\lambda_n} = \frac{(-1)^{\lambda_2+\cdots+\lambda_r}\ \lambda_{2i+1}(\rho-2i-1)(\lambda_1+\cdots+\lambda_n-2)!}{\lambda_1!\,\lambda_2!\cdots\lambda_n!}$$

. . . .

以上を交互に $+-$ すると $a_{\lambda_1,\cdots,\lambda_n}$ になる。よって定理が成り立つ

Sm. 5　°　$(k_1,\cdots,k_h)=\Sigma\, x_1^{k_1}\cdots x_h^{k_h}$
とおいて $1,2,\cdots,h$ の代わりに $1,2,\cdots,n$ の相異る項をもつ順列に Σ がわたるものとする。この時次の式が成り立つ。

$$(k_1,\cdots,k_h)(m) = c_1(k_1+m,k_2,\cdots,k_h)+c_2(k_1,k_2+m,\cdots,k_h)+\cdots + c_h(k_1,\cdots,k_h+m)+c_0(k_1,\cdots,k_h,m)$$

但し係数 c_i ($i=1,\cdots,h$) と c_0 は，その次にくる記号の中に，どれだけ k_i+m 又は m に等しい整数があるかを表わす。（但し形の同じものは省く）

第4章 §26

[証明] $(k_1,\cdots,k_n)(m)=(\sum_{s=1}^{n}x_s^m)(\sum x_1^{k_1}\cdots x_n^{k_n})$

ここで $k_1,\cdots,k_n$ のうち m に等しいものを c_0 個とし後の $(k_{(1)},k_{(2)},\cdots,k_{(p)})$ は $\sum$ の変数以外すべての順列にわたるものとすれば

$$(k_1,\cdots,k_n)(m)=\left\{\sum_{s=1}^{n}x_s^m\right\}\left\{\sum x_1^m\cdots x_{c_0}^m\right\}(k_{(1)},k_{(2)},\cdots,k_{(p)})$$

($k_{(1)}\cdots k_{(p)}$ は $k_1\cdots k_n$ の中で m と等しくないもの)

右辺の積を x_s を第2.3項中に含むものと含まないものに分けて

$$(k_1,\cdots,k_n)(m)=\sum_{s=1}^{m}\left(x_s^m\left(\sum_{p=1}^{\alpha}x_s^{k_p}(k_1,\cdots,k_{p-1}\,k_{p+1},\cdots,k_n)\right)\right)$$

$$+\sum_{s=1}^{m}\left(x_s^m\sum{}'(k_1,\cdots,k_n)\right)$$

但し $\sum'$ は $1,\cdots,n$ から s を除いたすべての順列にわたるとする。

一方

$$(k_1,\cdots,k_p+m,\cdots,k_n)=(\sum x_1^{k_p+m}\cdots x_{c_p}^{k_p+m})\,M_p$$

$$(k_1,\cdots,k_n,m)=(\sum x_1^m,\cdots,x_{c_0}^m)\,M_0$$

である。前の式は

$$(k_1,\cdots,k_n)(m)=\left(\sum_{p=1}^{\alpha}\sum_{s=1}^{n}x_s^{m+k_p}\sum{}'x_1^{m+k_p}\cdots x_{c_p-1}^{m+k_p}M_{ps}\right)$$

$$+\left(\sum_{s=1}^{m}x_s^m\sum{}'x_1^m\cdots x_{c_0-1}^m M_{0s}\right)$$

ここで M_{ps} M_{0s} 等は $\sum'$ の変数と x_s を抜いた変数にわたる。

つまり $1\sim n$ から c_p 個を除いた変数で指数に $m+k_p$ をもたないものからなる。即ち s を $1\sim n$ のすべての変数にとれば M_{ps} の各項は M_p の各項に一致する。即ち M_p のうち s を含まないもの全体が M_{ps} となる。以上と $\sum_{s=1}^{n}x_s^{m+k_p}\sum'x_1^{m+k_p}\cdots x_{c_p-1}^{m+k_p}$ が $\sum x_1^{k_p+m}\cdots x_{c_p}^{k_p+m}$ と c_p 回重複するから結局定理が成り立つ。

上の証明はあいまいな点が多く次にあらためて証明する

まず $(k_1,\cdots,k_n)$ は明らかに $k_1,\cdots,k_n$ の順序によらないから同じものを並べて書き直す $(k_1,k_1,\cdots k_p,k_p,\cdots k_p,\cdots\cdots,k_s)$ k_1 の個数を $f(k_1),\cdots,$ k_p の個数を $f(k_p)$ で表わす $x_1,\cdots,x_n$ から r 個とってできた積 $x_{i_1}\cdots x_{i_r}$ のすべての組合わせを

$$\sum P_r$$

と書く。$x_{i_1},\cdots,x_{i_r}$ の k 乗のすべての組合わせを $\sum P_r^k$ と書く

この定義より

1. $\Sigma_1 P_r^k \Sigma_1' P_s^k = \binom{r+s}{r} \Sigma_1 P_{r+s}^k$

がただちに得られるがそのために $\Sigma_1, \Sigma', \cdots, \Sigma_1^s$ を定義する。

$x_1, \cdots, x_n$ のうちから r 個とったすべての組合わせ

$\Sigma_1 P_r$

の各項 $x_{i_1} \cdots x_{i_r}$ を $x_1 \cdots x_n$ からぬいてできるうちからの s 個の全組合を ΣP_r の各項にかけ合わす演算を

$\Sigma_1 P_r \Sigma' P_s$ と

と書く（$\Sigma P_r \cdot \Sigma P_s$ とは区別する）

とうすれば例は $r=1$ として k 乗にて ΣP_1^k 即ち $\sum_{i=1}^{n} x_i^k$ と $\Sigma' P_r^j$ との積は

$$\Sigma P_1^k \Sigma' P_r^k = \sum_{i=1}^{n} \left\{ x_i^k \Sigma' P_r^j \right\}$$

で表わせる。更に

2. $\Sigma P_r^k \Sigma' P_s^j = \Sigma P_s^j \Sigma' P_r^k$ （定義より明らか）

3. $(k_1 \cdots k_s) = \Sigma P_{f(k_1)}^{k_1} \Sigma' P_{f(k_2)}^{k_2} \cdots \Sigma^{s-1} P_{f(k_s)}^{k_s}$

が成り立つ。次に

4. $(\Sigma P_1^m)(\Sigma P_{f(k_1)}^{k_1} \Sigma' P_{f(k_2)}^{k_2} \cdots \Sigma^s P_{f(k_s)}^{k_s})$

$$= \Sigma_1 P_1^m \Sigma' P_{f(k_1)}^{k_1} \cdots \Sigma^s P_{f(k_s)}^{k_s}$$

$$+ \sum_{i=1}^{n} \left\{ x_i^m \cdot \sum_{k=k_1}^{k_s} x_i^k \Sigma' P_{f(k)-1}^k \Sigma'' P_{f(k_1)}^{k_1} \cdots \Sigma^s P_{f(k_s)}^s \right\}$$

（2より因数の交換を行ない $P_{f(k)-1}^k$ を前に出した）

が成り立つ

$(m)(k_1 k_1 \cdots k_s)$ は 4 より

$\Sigma_1 P_1^m \Sigma' P_{f(k_1)}^{k_1} \cdots \Sigma_1^s P_{f(k_s)}^{k_s}$ と $\sum_{k=k_1}^{k_s} \left\{ \sum_{i=1}^{m} x_i^{k+m} (\Sigma_1' P_{f(k)-1}^k \cdots \Sigma_1^s P_{f(k_s)}^{k_s}) \right\}$

の和になる。まず前者は m に等しい k_1 の項を前に出して

$\Sigma_1 P_1^m \Sigma' P_{f(k_1)}^m \Sigma'' P_{f(k_1)}^{k_1} \cdots \Sigma^s P_{f(k_s)}^{k_s}$

の形にすれば 1. よりこれは

$(f(k_1)+1) \Sigma_1 P_{f(k_1)+m}^m \Sigma' P_{f(k_1)}^{k_1} \cdots \Sigma^{s-1} P_{f(k_s)}^{k_s}$

これはちょうど $(f(k_1)+1)(m, \cdots, m \; k_1 k_1 \cdots k_s)$

即ち $C_0(k_1 \cdots k_n \; m)$ に等しい。後者は前に述べたことから

5. $\sum_{k=k_1}^{k_s} \left\{ \Sigma P_1^{k+m} \Sigma' P_{f(k_1)}^{k_1} \Sigma'' P_{f(k_2)}^{k_2} \cdots \Sigma^s P_{f(k_s)}^{k_s} \right\}$ となる

前者と同様に $k+m$ に等しい k_j をきめ それを使って書き直すと

$$\sum_{k=k_1}^{k_s}\left\{(f(k_j)+1)\sum P_{1+f(k_j)}^{k+m}\ \sum{}' P_{f(k_j)-1}^{k+m}\ \sum{}'' P_{f(k_1)}^{k_1}\cdots\sum P_{f(k_s)}^{k_s}\right\}$$

積を $k_1,\cdots,k_s$ の順に直すと

$$\sum_{r=1}^{s}\left\{ C_r \sum P_{f(k_1)}^{k_1}\cdots\cdots\sum^{r-1} P_{f(k_r)-1}^{k_r}\cdots\sum^{j-1} P_{C_r}^{k_r+m}\cdots\cdots\sum^{s-1} P_{f(k_s)}^{k_s}\right\}$$

即ち $\displaystyle\sum_{r=1}^{s} C_r(k_1,\cdots,k_r+m,\cdots k_s)$ となる。よって定理は証明された。

注）§27.28 終結式はは行列で扱ったので省く。

§29 有理函数の部分分数分解

定理 ○ 互いに素な，体K上の多項式を $g(x)$，$h(x)$ とし，$g(x)$ の次数を a，$h(x)$ の次数を b とする。$f(x)$ を次数が $a+b$ よりも低になってる多項式とすると等式

$$f(x) = r(x)\,g(x) + s(x)\,h(x)$$

を満たす $r(x)$（次数 $<b$）．$s(x)$（次数 $<a$）が存在する。

（証明） $(g(x), h(x)) = 1$ だから．

$$1 = c(x)\,g(x) + d(x)\,h(x)$$

を満たす，$c(x)$．$d(x)$ が存在する。両辺に $f(x)$ を乗ずると

$$f(x) = f(x)c(x)\,g(x) + f(x)d(x)h(x)$$

$$f(x)c(x) = h(x)\,P(x) + r(x). \qquad r \text{ の次数} < b$$

とすると

$$f(x) = r(x)\,g(x) + \bigl(g(x)P(x) + f(x)d(x)\bigr)\,h(x)$$

左辺及び右辺の第1項の次数は $a+b$ より小さいから右辺の第2項も次数は $a+b$ より小さく したがって $g(x)P(x)+f(x)d(x)$ の次数は a よりも小さい。$g(x)P(x)+f(x)d(x) = s(x)$ とおけばよい。 QED

$$f(x) = r(x)g(x) + s(x)h(x)$$

を $g(x)h(x)$ でわれば

1. $$\frac{f(x)}{g(x)h(x)} = \frac{r(x)}{h(x)} + \frac{s(x)}{g(x)}, \quad \begin{array}{l}\alpha(r) < \alpha(h) \\ \alpha(s) < \alpha(g)\end{array}$$

（αは次数）

2. $$\frac{f(x)}{p(x)^m} = \frac{r_1(x)}{p(x)} + \frac{r_2(x)}{p(x)^2} + \frac{r_3(x)}{p(x)^3} + \cdots + \frac{r_m(x)}{p(x)^m}$$

但 $\alpha(f) < m\alpha(p)$ $\alpha(r_i) < \alpha(p)$ $(i = 1, \cdots, m)$

（証明） $\alpha(p) = p$ とおいて.

$$f(x) = p(x)^{m-1} r_1(x) + s_1(x), \quad \alpha(s_1) < (m-1)\alpha(p), \ \alpha(r_1) < p$$

$$s_1(x) = p(x)^{m-2} r_2(x) + s_2(x), \quad \alpha(s_2) < (m-2)\alpha(p), \ \alpha(r_2) < p$$

$$s_2(x) = p(x)^{m-3} r_3(x) + s_3(x), \quad \alpha(s_3) < (m-3)\alpha(p), \ \alpha(r_3) < p$$

$$\cdots\cdots\cdots\cdots$$

$$s_{m-1}(x) = p(x)^0 r_m(x) + s_m(x), \quad s_m = 0, \ \alpha(r_m) < p.$$

それぞれを前の式に代入していき最後に両辺を $p(x)^m$ でわる。 QED

第 5 章 体 論

§ 30 部分体，素体

1. 部分体 …… 斜体 Σ の部分集合 Δ が又斜体である． Δ

条件（必要十分） …… Δ が 0 以外の要素 a, b を含み，a, b を含めば $a-b$ ab^{-1} も含む。

① 部分体 M, N の共通集合 Δ はやはり部分体である。

2. 素体 …… 斜体 Σ の全部分体の共通集合を Σ の素体という。

（正確には真の部分体をもたない Σ の部分体）

3. 素体の型 … Σ に含まれる素体を Π とする。

$$0 \in \Pi, \quad e \in \Pi \qquad ne \in \Pi \quad (n \text{は整数})$$

$$ne + me = (n+m)e$$
$$ne \cdot me = nm \cdot e$$

∴ 単位要素の整数倍 ne は可換体 P を作る。

写像 $f : n \to ne$

は有理整数環 Z から P へ準同型写像を与える。

$$Z/\mathfrak{p} \cong P$$

1. $\mathfrak{p} = (p)$， p は素数

$$P \cong Z/\mathfrak{p}$$

∴ $P = \Pi$

2. $\mathfrak{p} = (0)$， P の商体を Q とすれば

$$Q = \Pi$$

4 標数 … p． 1 の場合は (p) の p，2 の場合は 0

T. 1. ◦ Σ の標数を k とし，$a \neq 0$ を Σ の要素とすると，$na = ma$ であるためには $n \equiv m \ (k)$ であることが必要十分である。

T. 2. ◦ 標数 p の可換体においては

$$(a+b)^p = a^p + b^p$$
$$(a-b)^p = a^p - b^p$$

Sm1. 標数 p の体に於ては

$$(a+b)^{p^f} = a^{p^f} + b^{p^f}$$

(証明) $f=1$ の時 $(a+b)^p = a^p + b^p$ は明らかに成り立つ。

$f=k$ の時

$$(a+b)^{p^k} = a^{p^k} + b^{p^k}$$

が成り立つとする。すると

$$(a+b)^{p^{k+1}} = ((a+b)^{p^k})^p = (a^{p^k} + b^{p^k})^p = a^{p^k \cdot p} + b^{p^k p} = a^{p^{k+1}} + b^{p^{k+1}}$$

故に定理は成立する。

Sm2 標数 P の体に於ては

$$(a_1 + a_2 + \cdots + a_m)^p = a_1^p + a_2^p + \cdots + a_m^p$$

(証明) $m=2, 1$ の時成り立つ。

$m=k$ の時 $(a_1 + a_2 + \cdots + a_k)^p = a_1^p + \cdots + a_k^p$

が成り立つとすれば

$$(a_1 + a_2 + \cdots + a_k + a_{k+1})^p = (a_1 + a_2 + \cdots + (a_k + a_{k+1}))^p$$

$$= a_1^p + a_2^p + \cdots + a_{k-1}^p + (a_k + a_{k+1})^p$$

$$= a_1^p + a_2^p + \cdots + a_k^p + a_{k+1}^p$$

故に定理は成立する。

Sm3 整数環に於て P を素数とすれば

$$a^p \equiv a \mod p$$

(証明) 剰余環 Z/p は明らかに体で $pe \equiv 0 \mod p$ だから明らかにその標数は p §2 の式に於て $a_1 = a_2 = \cdots = a_m = 1$ とおけばよい。

注) $a^p \equiv a \mod p$ $\therefore$ $a(a^{p-1} - 1) \equiv 0 \mod p$

$a \not\equiv 0 \mod p$ ならば $a^{p-1} \equiv 1 \mod p$ (フェルマーの定理)

Sm4 標数 P の時

$$(a-b)^{p-1} = \sum_{\delta=0}^{p-1} a^\delta b^{p-1-\delta}$$

(証明) $(a-b)^p = a^p - b^p$

$$a^p - b^p = (a-b)(a^{p-1} + a^{p-2}b + \cdots + b^{p-1})$$

a, b を不定元と見るに

$$(a-b)^p = (a-b)(a^{p-1} + a^{p-2}b + \cdots + b^{p-1})$$

の両辺を $(a-b)$ で除いて定理を得る。

第5章 §31

Sn5 ガウスの整数環 $Z[i]$ で、素イデアル $(1+i)$，(3)，$(2+i)$ を法とする剰余類の標数はいくらか。

（解答）

① $Z/(1+i)$ は $2\equiv 0 \mod (1+i)$ だから 標数は 2

② $Z/3$ は $3\equiv 0 \mod 3$ だから 標数は 3

（ $2\not\equiv 0 \mod 3$，$1\not\equiv 0 \mod 3$ ）

③ $Z/(2+i)$ は $5\equiv 0 \mod (2+i)$ だから 標数は 5

§31 付 加

定義 ◦ 1. 体 Δ が体 Ω の部分体の時 … $\Omega \to \Delta$ の拡大体

◦ 2. Δ の拡大体 Ω が存在するとする，Ω の部分集合 M と Δ を含むあらゆる体の共通集合を $\Delta(M)$ … Δ に M を付加した体

◦ 定義より $\Delta \subseteq \Delta(M) \subseteq \Omega$

定理 ◦ 1 $M = M_1 \cup M_2$ ならば $\Delta(M) = \Delta(M_1)(M_2)$

（証明） $\Delta(M_1)(M_2) \supseteq \Delta, M_1, M_2$

$\therefore\ \Delta(M_1)(M_2) \supseteq \Delta(M)$

$\Delta(M) \supseteq \Delta, M_1, M_2$ $\because$ $\Delta(M) \supseteq \Delta(M_1), M_2$

$\therefore\ \Delta(M) \supseteq \Delta(M_1)(M_2)$ QED

以上より $\Delta(M) = \Delta(M_1)(M_2)$

◦ 単純拡大 付加する M の位数が 1 即ち Ω のただ1つの要素である場合，$M=\{a\}$，として $\Delta(a)$ と書く。

注）体 Δ に環の付加をする時には $\Delta[a]$ と書く。

§ 32. 単純拡大

以下体はすべて可換とする。又 Δ, Ω は体で $\Delta \subseteq \Omega$ とする。

証明を抜いて定理だけを上げる。

定理 ◦ ◦ Δ の単純拡大体には，代数的なものと超越的なものとがある。

前者の場合

Ωの付加する要素ϑに対して1つの多項式$\varphi(x)$が存在し

$\varphi(\vartheta)=0$ （$\varphi(x)=0$ を定義方程式という。

で $\Delta(\vartheta)\cong\Delta(x)/(\varphi(x))$

次数 が成り立つ。 注）φはΔの要素を係数としφの次数をϑのΔに関する次数という。

尚この対応は $\sum a_k\vartheta^k\to\sum a_k x^k$ で行なわれる。

後者の場合 Ωの付加する要素ϑは不定元と同一視され

$\Delta(\vartheta)\cong\Delta(x)$

$\Delta(x)$はΔ上の1変数有理函数体とする。対応は$\vartheta\to x$

S.1 次の拡大の生成要素の次数 定義方程式を求めよ

a) 実数体Rに関して，複素数C

b) 有理数体Pに関して，体$P(\sqrt{3})$

c) 有理数体Pに関して，体 $P\left(e^{\frac{2\pi i}{5}}\right)$

（解答）

a) 2次 $f(x)=x^2+1$

b) 2次 $f(x)=x^2-3$

c) 4次 $f(x)=x^4+x^3+x^2+1$

○ d) 体$Z[i]/(7)$，その中に含まれる素体に関して

（解答） 単位要素 1 は $7\cdot 1=$ ではじめて 0 になるから

素体は (7) である。この場合も生成要素はiで定義方

程式は $x^2+1=0$ である。（-1 は7の平方剰余類ではない）

S.2 Γは可換な基礎体とし，zは不定元として，$\Sigma=\Gamma(z)$，$\Delta=\Gamma\left(\frac{z^2}{z+1}\right)$ とおく。

この時 Σ/Δは，単純拡大であることを示せ． 要素zがみたすΔの既約多項式はどうなるか。

（証明） $\frac{z^2}{z+1}\in\Delta$ だからzは $z^2-\alpha(z+1)=0$ （αはΔの要素）

を満たす。Δに方程式 $z^2-\alpha z-\alpha=0$ の根を付加すればよい。

zが$\Gamma\left(\frac{z^2}{z+1}\right)$に含まれていることはない。もし含まれていたとすると zがΔの要素

即ちΓの要素を係数とする方程式を満足することになる。

故に Σ/Δは単純拡大体である。

第5章 §32

○ 同型

体Δの2つの拡大体 Σ Σ' が同型とは

Δの要素をΔ自身の要素に移す同型 $\Sigma \cong \Sigma'$ が存在する。

* 単純超越的拡大はみる同型である。

* 2つの単純代数的拡大 $\Delta(\alpha)/\Delta$、$\Delta(\beta)/\Delta$ は α, β が $\Delta[x]$の同一の既約多項式 $\varphi(x)$の根であれば同型である。

* Δ上同型な拡大体が、共通の拡大体Ωに含まれている時、これらはたがいに、Δ上で共役であるという。

共役

* $\Delta[x]$の既約多項式のΩにおける根すべて、Δ上で互いに共役である。

又 代数的に共役な要素は、同じ既約多項式の根である。