NOTE BOOK

CONTAINING BEST RULED FOOLSCAP

代数学

I

No. 25

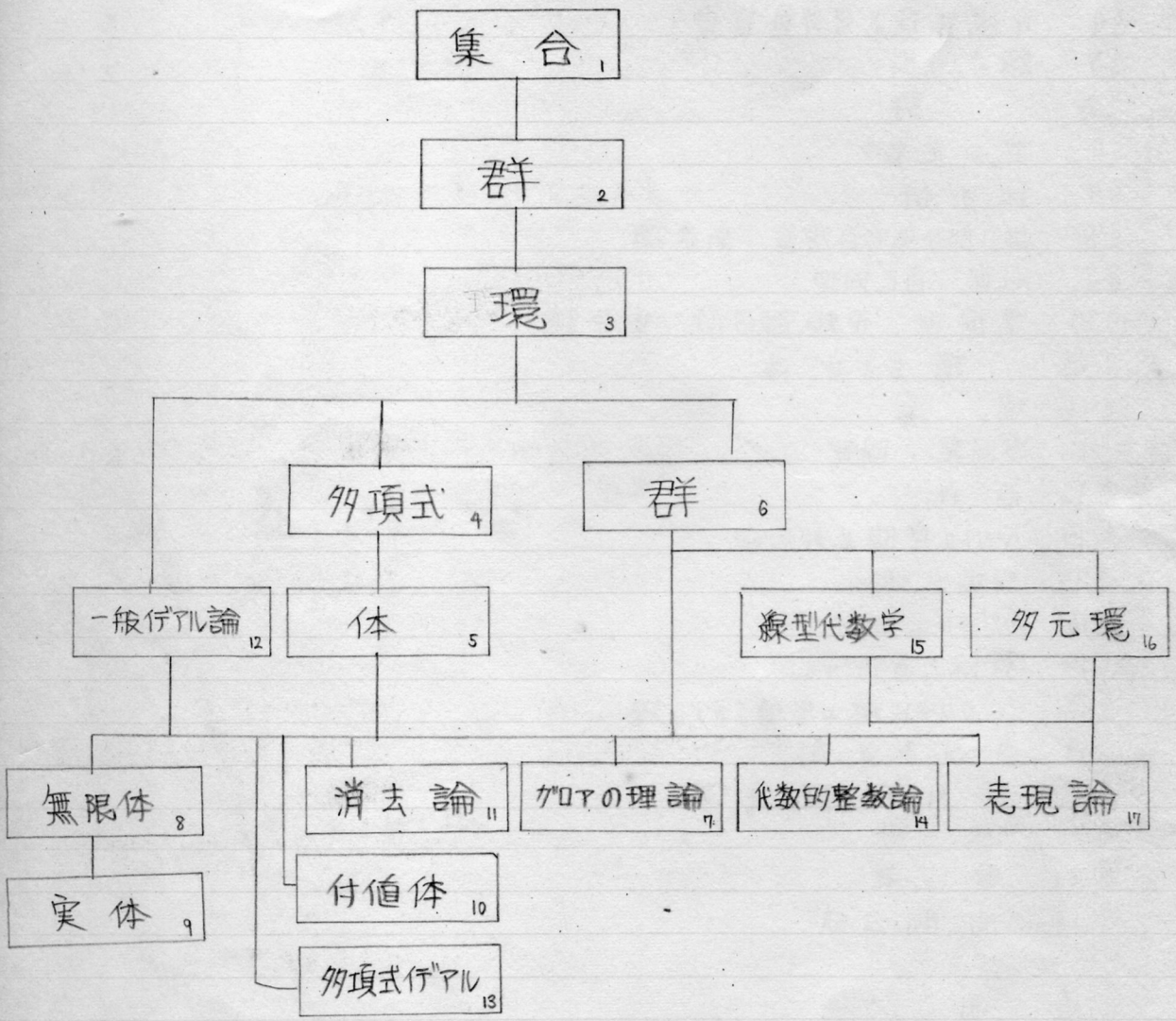
洛北

猪瀬博司

目　次

プログラム

下図は本ノートの構成を示したもの.



第1章 数と集合

§1. 集合

集合

○ 集合 …… 数学的思考の出発点としての 表象できるいろかの〈もの〉の内ある性質をもつものの集まり（あるいはもたない〈もの〉）を集合又は類という。（内包的定義）。（例，数や，文字も〈もの〉とみなすことができる。）

要素

〈もの〉 a が 集合 M に属す時，a を集合 M の要素といい，

$$a \in M$$

空集合

なる記号で表わす。（要素の一つもない集合を空集合という。）

注） 集合自体があるたなる集合をつくることがある。

部分集合

○ 集合 N のすべての要素が，M の要素にもなっている時 N を M の部分集合といい，

$$N \subseteq M$$

拡大集合

で表わす。この時 M を N の上集合，又は拡大集合といい

$$M \supseteq N$$

で表わす。 $A \subseteq B$，$B \subseteq C$，ならば $A \subseteq C$ である。
又 N が M の部分集合（拡大集合）で 且つ M が N の部分集合（拡大集合）の時 集合 N，M は等しいといい。 $M=N$ で表わす。

真部分集合
真拡大集合

$N \neq M$ で $N \subseteq M$ の時，N を M の真部分集合といい，$N \subset M$ と書く。
この時 M を N の真拡大集合といい，$M \supset N$ と書く。

共通集合

○ 集合，A，B に共通なすべての要素の集合を A，B の共通集合といい，
共通集合 D は

$$D = [A, B] = A \cap B$$

とかく。又 A，B 少なくともどちらか一方に含まれているすべての要素の集合を，A，B の合併集合といい，合併集合 V は

合併集合

$$V = A \cup B$$

で表わされる。上と同様なことが，集合，A，B，… の集合，Z についても定義される。集合 $D = A \cap B$ が空集合の時，A，B は互いに無縁であるという。

互いに無縁

第1章 第1節～第2節～第3節

○ 集合を表わすのに、その要素を列挙してもよい。集合 M が a, b, c より成る時は

$$M = \{a, b, c\}$$

と書く（外延的定義）この時この集合の要素を定義する性質は
〈a, b, c のいずれかに一致する〉ということである。

写像
濃度
函数
定義域
値域

§2. 写像、集合の濃度

○ 函数 …… 集合 M の各要素 a に1つの《もの》$\varphi(a)$ が対応させられている時この対応を函数という。集合 M を その函数の定義域、$\varphi(a)$ の集合 N をその函数の値域という。

○ 写像 …… 集合 M の各要素に集合 N の要素がただ1つ対応し、且つ N の要素がすべてつくされるような函数を集合 M から集合 N への写像という。
$\varphi(a)$ を a の像、a を $\varphi(a)$ の原像という。
又 a にただ1つ $\varphi(a)$ が対応し、$\varphi(a)$ にただ1つ a が対応する時、この対応を逆一意又は1対1であるという。2つの集合 M, N にこのような対応がつく時、集合 M, N は対等であるといい、

$$M \sim N$$

で表わす。対等な集合は等しい濃度をもつという。

1対1

1. $A \sim A$　2. $A \sim B$ ならば $B \sim A$　3. $A \sim B$、$B \sim C$ ならば $A \sim C$

§3. 自然数列

ペアノの公理

○ ペアノの公理

Ⅰ　1は自然数である。

Ⅱ　各数 a に対してただ1つの後者 a^+ が自然数中に存在する。

Ⅲ　$a^+ \neq 1$.

Ⅳ　$a^+ = b^+$ ならば $a = b$

Ⅴ　自然数の集合が、数1を含み、数 a を含むと仮定した時 a^+ をも含むものとする。するとこの集合は自然数全体である。

数学的帰納法

注）Ⅴによって一般の数学的帰納法による証明が可能になる。

和

○ 和　任意の数 x, y に対して，自然数 $x+y$ がただ1つ対応する。

(1) 任意の x に対して　$x+1 = x^+$

(2) 任意の x と y に対して　$x+y^+ = (x+y)^+$

結合法則 交換法則

(3) $(a+b)+c = a+(b+c)$　（結合法則）

(4) $a+b = b+a$　（交換法則）

(5) $a+b = a+c$ ならば　$b = c$

積

○ 積　任意の数 x, y に対して，自然数 $x \cdot y$ あるいは xy がただ1つ対応する。

(6) 任意の x に対して　$x \cdot 1 = x$

(7) 任意の x, y に対して　$x \cdot y^+ = x \cdot y + x$

(8) $ab \cdot c = a \cdot bc$　（結合法則）

(9) $a \cdot b = b \cdot a$　（交換法則）

(10) $a(b+c) = a \cdot b + b \cdot c$　（分配法則）

(11) $ab = ac$ ならば　$b = c$

注）{ でくくったのは演算法則

大小

○ 大小　$a = b+u$ の時 $a > b$ または $b < a$ と書くこれについて次が成り立つ。

(12) 各2数 a, b に対して

$a < b$,　$a = b$,　$a > b$

のうち1つが成り立つ。

(13) $a < b$, $b < c$ ならば　$a < c$

(14) $a < b$, ならば　$a+c < b+c$

(15) $a < b$, ならば　$ac < bc$

$a > b$ の時方程式 $a = b+u$ の解 u［(5)によってただ1つ存在］を，$a-b$ と書く。$a < b$ あるいは $a = b$ ということを $a \leqq b$ と略記する 同様に $a \geqq b$ も定義される。

最小自然数

○ 空でない自然数の集合は最小数を含む　（最小自然数の存在）

この定理によって数学的帰納法の第2の型が得られる。

▷ ある性質Eがすべての n より小さいすべての数に対して成り立つという仮定の下で Eが n に対して成り立つならすべての自然数が性質Eをもつ。

注）$n=1$ の時仮定が成り立たないが，空集合はすべての性質E，…，をもつと仮定しておけば（これはかえって好都合なことが多い）当然 $n=1$ の時性質Eが成り立つのを示さなければならない。この定理は上述の最小自然数の存在より容易に証明できるので証明は省く。

第1章 第3節

○ 数学的帰納法による定義

各自然数に《もの》 $\varphi(a)$ を対応させ，これが前もって与えられた《帰納的関係》をみたすようにする。（$m<n$ なる 函数値 $\varphi(n)$ が $\varphi(m)$ に対して一定の関係を満足させるようにする）ここでは特に $m<n$ なる $\varphi(m)$ によって $\varphi(n)$ が一意的に決定されるような函数を扱う。（ただし $\varphi(1)$ はあらかじめ定めておく）

▷ 定理 ◁ 上にのべたような仮定が与えば，与えられた関係を満たす 函数 $\varphi(x)$ が1つ，しかもただ1つ存在する。

切片

［証明］ $x \leqq n$ を満たす数 x の全体を自然数の切片とよび $(1, n)$ であらわす まず与えられた関係を満たす切片 $(1, n)$ 上の函数が，1つ，しかもただ1つ存在することを証明する。まずこれは切片 $(1, 1)$ に対して成り立つ。切片 $(1, n)$ について成り立てば 切片 $(1, n^+)$ についても成り立つ（$\varphi(n^+)$ は $m<n^+$ の $\varphi(m)$ 即ち $(1, n)$ の m によって一意的に決定される。）よってこの主張はすべての切片 $(1, n)$ で成り立つ。又明らかに $\varphi_n(x)$ は $m<n$ なる切片 $(1, m)$ 上で $\varphi_m(x)$ と一致する。従って各々の $\varphi_k(x)$ はそれらの定義域内の x においては一致する。求める函数は，どの切片 $(1, n)$ 上においても定義されていて，決定関係を満たすから $(1, n)$ 上で $\varphi_n(x)$ に一致しなければならない。このような函数は存在し，しかもただ1つである。即ち その値 $\varphi(x)$ を数 x において定義されるすべての $\varphi_n(x)$ の共通の値とすればよい，又そうしなければならない。これで定理は証明された。

例題

1. ある性質 E が $n=3$ に対して成り立ち $n \geqq 3$ に対して成り立つなら $n+1$ に対しても成り立つとすると，E はすべての数 $\geqq 3$ に対して成り立つ。

（証明） 性質 E が成り立たないような $m \geqq 3$ が存在したとし それらすべてからなる集合を M とする。M は仮定より空集合ではない。よって M には最小自然数 a が存在する（$a>3$） a より小さい数は当然皆性質 E を有するところが a を後者としてもつ数 即 $a-1$ は性質 E を有する。ところが，仮定より $(a-1)+1=a$ も又性質 E をもつことになり，明らかにこれは不合理である。よって与定理は成り立つ。

整数

○ 整数

自然数の組 (a, b) を新しい対象と見なし，次のように演算を定義する。

I $(a, b)+(c, d)=(a+c, b+d)$

II $(a, b)\cdot(c, d)=(ac+bd, ad+bc)$

III $a+d<b+c$ の時 $(a, b)<(c, d)$ 又は $(c, d)>(a, b)$

このように定義された数の対を整数と名付ける。

これを 正数 $a=(a+b, b)$，負数 $-a=(b, a+b)$

$0=(b,b)$ という形に直した記法が通常整数とよばれているものである。整数に於ては減法（即ち $a=b+x$ なるxを求める算法）を無制限に行なうことができる。又 整数に於ては $ab=0$ になるのは、$a=0$ か $b=0$ の時だけである。

（証明）

まず $a=0$ 又は $b=0$ の時 $ab=0$ を証明する。

$a=(a_1,a_2)$, $b=(b_1,b_2)$ とする。

すると $a_1=a_2$ かつ又は $b_1=b_2$ の時

$$(a_1,a_2)\cdot(b_1,b_2)=(a_1b_1+a_2b_2,\ a_1b_2+a_2b_1)$$

$$=\left\{\begin{array}{l}(a_1(b_1+b_2),\ a_1(b_1+b_2))\\(b_1(a_1+a_2),\ b_1(a_1+a_2))\end{array}\right\}=0$$

次に $ab=0$ ならば $a=0$ か $b=0$ であることを証明する。

$$a_1b_1+a_2b_2=a_1b_2+a_2b_1$$

の時もし $a\neq 0$, $b\neq 0$. 即ち $a_1\neq a_2$, $b_1\neq b_2$ とする。

ここで $a_1>a_2$, $b_1\neq b_2$ の時のみを考えるその他の時も全く同様にすればよい。 $a_1>a_2$ であるから、

$$b_1(a_1-a_2)=b_2(a_1-a_2)$$

$$\therefore\quad b_1=b_2 \quad\rightarrow\ 不合理$$

○ 整数に於ても 演算規則 (3), (4), (5), (6), (9), (10), (12), (13), (14) が成り立つ。(15) も $c>0$ に対して成り立つ。

§4 有限集合と可付番集合

有限集合

○ 有限集合 …… 自然数の切片と対等な集合（空集合も含める）

有限集合はその要素に1からnまでの番号をつけ、各々に異なった番号がつくように、1からnまでの番号がつくされるようにできる集合のことである。

$$A=\{a_1,a_2,\cdots,a_n\}\qquad(Aは有限集合)$$

と表わすことができる。

sn 1.

○ 有限集合の部分集合は又有限集合である。

✗[証明] 切片 $(1,1)$ に対等な集合には明らかに成り立つ。今 $n-1$ に

対して定理が成り立つとする。

$A_m = \{a_1, \cdots, a_m\}$

の任意の部分集合をBとする時 Bは A_m の真部分集合か A_m 自身に等しい。後者の場合 Bは当然有限集合である。さてBを A_m の真部分集合であるとすると A_m に属しBに属さないような要素cが少なくても1つ存在する。(このような要素を a_i とする) A_m から a_i を除いた集合 A_{m-1} は明らかに切片 $(1, m-1)$ と対等である 又Bは明らかに A_{m-1} の部分集合だから与定理はすべてのnについて成り立つ。

無限集合

注) 有限集合でない集合を無限集合という。

▷有限集合の基本定理◁

有限集合がその真拡大集合と対等になることはない。

[証明] 有限集合Aからその真拡大集合への写像があったと仮定する。

$A = \{a_1, a_2, \cdots, a_m\}$ とすると Bへの像 $\varphi(a_1), \varphi(a_2), \cdots, \varphi(a_m)$ 中には $a_1, \cdots, a_m$ が含まれ更にそうでない《もの》も少なくても1つ含まれているそれを a_{m+1} とする。$n=1$ の時与定理は成り立つ。$n=m$ の時与定理が成り立っていると仮定する。さてここで $\varphi(a_m) = a_{m+1}$ としてよい。(写像の変形) そうすると、Aの部分集合 $A' = \{a_1, \cdots, a_{m-1}\}$ の写像 $\varphi(A')$ はAを含むこれは帰納法の仮定により不可能である。

系 自然数列の2つの切片 $(1, n), (1, m)$ が $n \neq m$ で対等になることはない。

注) 有限集合はある切片 $(1, n)$ に対等で系により $n \neq m$ なる $(1, m)$ には対等でない よって1つの有限集合が与えられるとそれによって n なる数が一意的にきまる。これを有限集合の要素の個数という。(空集合の時は $n=0$ とする)

個数

○ 自然数全体の集合は いかなる切片 $(1, n)$ に対しても対等でない。よって無限集合である。又自然数列に対して対等な集合を可付番集合という。要素に自然数の番号を1回ずつつけることができる。

可付番集合

注) この場合自然数列は自然数全体も含んでいるとする。

Sn 2. ○ 2つの互いに無縁な有限集合の合併集合の要素の個数はもとの2つの集合の要素の個数の和に等しい。

(証明) まず集合Aの個数が n Bの個数が1の時はBの要素に n^+ なる自然数との対応を与えればよい。$n^+ = n+1$ だからBの個数が1の時は定理は成り立つ。集合Bの個数が m の時与定理が成り立つとする。

集合Bの個数を m^+ とし 集合Bのうち1個を除いて集合B'をつくると その個数は当然 $n+m$ である。次に残りの1個に自然数 $(n+m)^+$ を対応させる。すると 結局 AUB は $(n+m)^+$ の個数をもつことになる。$(n+m)^+ = n+m^+$ より 5定理は証明された。

sn.3. ○ それぞれ S 個の要素をもつ、r個の互いに無縁な集合の合併集合の要素の個数は sr に等しい。

(証明) まず $r=1$ に対しては5定理は正しい。$r=m$ の時5定理は正しいとする。$r=m^+$ の時この中の m 個については定理は成り立つ。あとの1個の集合と sm の個数をもつ集合の合併集合の個数は sn 2 より $sm+S$ である。ところが $sm^+ = sm+S$ であるからこれは sm^+ に等しい。

sn 4 ○ 自然数列の部分集合は可付番である。

(証明) 大小の順に並らべて小さいものから順に 1, 2, ⋯, m ⋯ と対応させて行けばよい。

sn 4 系 集合が可付番なのはその集合の各要素に異なった番号をつけることのできる時にかぎる。

▷ 自然数のすべての可付番集合の集合は可付番ではない ◁

[証明] $A_i = \{ a_{i1}, a_{i2}, \cdots, \cdots \}$ とする。

ここで $B = \{ a_{11+1}, a_{22+1}, \cdots, a_{kk+1}, \cdots \}$ なる可付番集合をつくると B は可付番であるから例えば A_j と一致する。ところが、Bの第j番目の要素は a_{jj+1} であるのに、A_j の第j番目の要素が a_{jj} になって明らかにこれは不合理である。

sn 5. ○ 整数全体の集合Zは可付番である。

(証明) 正数 a には $2a$ を 負数 $-b$ には $2b+1$、0には1を対応させればよい。同様に偶数全体の集合も可付番である。

sn 6 ○ 実数全体の集合Rは可付番集合ではない。

(証明) 実数を0と1の間に限り、任意の数を $a_i = 0.a_{i1}a_{i2}\cdots$ で表わし a_i を $a_{i1}, a_{i2}, \cdots$ の集合とみなして上述の論法と同様にすればよい。

カントールの対角線論法

注) この論法を〔カントールの対角線論法〕という。

sn 7. ○ 可付番無限集合に有限個の、あるいは可付番個の新しい要素を追加しても その濃度は変わらない。

(証明) 追加する集合と交互に番号をつけていけばよい。

第1章 第4節～第5節

▷ 可付番集合の可付番個の合併集合は又可付番集合である◁

[証明] 集合を $M_1, M_2, \cdots$ とし M_i の要素を $m_{i1}, m_{i2}, \cdots$ とする
$i+k=S$ なる要素 m_{ik} は有限個しかない $S=2,3,\cdots$ としその各々に番号をつけて行けば $M_1 \cup M_2 \cup \cdots$ は可付番となる。

sn8 すべての既約分数 $\pm\frac{a}{b}$ (a,b は互いに素な自然数の集合は、可付番集合である。

[証明] 上の例にならい $a+b=S$ として $S=2,3,\cdots$ としてそれぞれに番号をつけて行き既約なものだけをとり出せばよい。

類別

§5 類別

等号

○ 等号の性質

反射的 I $a=a$ (反射的)

対称的 II $a=b$ ならば $b=a$ (対称的)

推移的 III $a=b$, $b=c$ ならば $a=c$ (推移的)

同値関係

○ 同値関係の定義

I $a \sim a$

II $a \sim b$ ならば $b \sim a$

III $a \sim b$, $b \sim c$ ならば $a \sim c$

類

○ 類 … 上で定義された同値関係によって、要素 a に同値な要素全体を1つの類 $C(a)$ にまとめることができる。この類 $C(a)$ のどの要素も $C(a)$ の代表になることができる。

○ 集合は、互いに無縁な類に分割される。

$a \sim b$ は $C(a)=C(b)$ と同じことである。

同値関係 $a \sim b$ は $C(a)=C(b)$ におきかえることができる。

集合 M が互いに無縁な類に分割され、a,b が同じ類に属する時 $a \sim b$ と定義すれば関係 $a \sim b$ は公理 I II III を明らかに満たす同値関係である。

群

第2章　群

§6 群の定義

1. 空でない集合 G の任意の2つの要素 a, b に対して第3の要素を対応させる結合関係を a, b の"積"と称し、ab 又は a·b と書く。
2. G の結合関係について結合法則が成立する。
$$a\cdot bc = ab\cdot c$$
3. G のすべての要素 a に対して
$$ea = a$$
単位要素　を満足させる単位要素 e が（少なくても1つ）G内に存在する。
4. G の各要素に対して
$$a^{-1}a = e$$
逆要素　という性質をもつ逆要素 a^{-1} が（少なくても1つ）G内に存在する。

アーベル群　注）　$ab = ba$ が成り立つ時 G は特にアーベル群［可換群］と呼ばれる。

可換群　"積"なる結合関係は和としても、何をとろうと自由。

◦ 群の例

① すべての有理数 … 乗法に関して群をつくる。
② 1と−1 … 乗法に関して群をつくる。
③ すべての整数 … 加法に関して群をつくる。
④[*1] 回転群 … 操作の連続を"積"とみなして群をつくる。　回転群
⑤[*2] 変換群 … 操作の連続を"積"とみなして群をつくる。　変換群

*1 回転群とは空間の回転を"もの"とみなしてそのすべての集合を上の積の定義によって定めた群

*2 変換群とは集合 M に集合 M 自身を対応させる函数全体の集合。
M が有限集合の時これを置換群と呼ぶことがある。　置換群

注）①～⑤が群であることの証明は省く

数加群　、加法に関に群をつくる数の集合を数加群と呼ぶ。

対称群　◦ 対称群

n個の要素からなる有限集合Mの置換全体を n次対称群という。

◦ 左単位要素と右単位要素は等しい。

∵ 3と4より　$a^{-1}aa^{-1} = ea^{-1} = a^{-1}$　左から a^{-1} の逆要素をかけると　$aa^{-1} = e$

第2章 第6節

除法の可能性

5. a, b を G の任意の要素とすると方程式 $ax=b$ と $ya=b$ は G 内に解をもつ

［証明］ $x=a^{-1}b$, $y=ba^{-1}$ がその解である。（除法の可能性）

除法の一意性

6 $ax=ax'$ あるいは $xa=x'a$ ならば $x=x'$ （除法の一意性）

［証明］ 両辺に左から a^{-1} を乗じて $x=x'$. 後者も同様

注）今まで述べた単位要素 e を 1 で表わすことも多い。

◦ 1.2.5 から 3. 4. が導ける。（群の定義II）

［証明］ G の一つの要素 c を選び 方程式 $xc=c$ を解を e と書く

即ち $ec=c$ かつてる a をとり 方程式

$cx=a$

を解くすると $ea=ecx=cx=a$ で3が証明された。

4の方は $xa=e$ が解けることに他ならない。

◦ 1, 2, 6 から 5 が導ける。（群の定義III）但し G は有限群

［証明］ 任意の要素を a とし各要素 x に ax を対応させる。この対応は1対1である。つまり積 ax は有限集合 G のすべてを尽くすよって すべての要素 b が $b=ax$ で表わされる。

位数

注）有限群の要素の個数を位数という。

▷ 群の定義 ◁

1. 結合関係の存在
2. 結合法則の成立
3. 単位要素の存在
4. 逆要素の存在

5 除法の可能性

6 除法の一意性

4 → 定義I

5 → 定義II

6 → 定義（有限群）III

◦ 演算規則

◦ $(ab)^{-1}=b^{-1}a^{-1}$

$\because$ $(b^{-1}a^{-1})ab=b^{-1}(a^{-1}a)b=b^{-1}eb=eb^{-1}b=e$

加群 モジュール

注）結合関係を加法的に書いた群を加群又はモジュールと呼ぶ。アーベル群はこの形で書くことが多い。

sn. l.

◦ 2つの要素 e, a は結合関係

$ee=e$, $ea=a$, $ae=a$, $aa=e$

によって可換群を作る。

〔証明〕

1 は明らか　又 $e(ee)=(ee)e=e$, $e(ea)=(ee)a=a$

$e(ae)=(ea)e=a$, $e(aa)=(ea)a=e$, $a(ee)=(ae)e=a$

$a(ea)=(ae)a=e$, $a(ae)=(aa)e=e$, $a(aa)=(aa)a=a$

より 結合法則も成立, 又 $ae=ea=e$, $ee=e$

より e は明らかに単位要素となる。又 $aa=e$, $ee=e$

より $a^{-1}=a$ 即ち 逆元が存在する。又これは明らかに可換であるから

加換群である。

Sn 2 群表

◦ 3次の対称群の群表（群の結合関係の表）を作れ.

要素を 1, 2, 3 とする. するとその対称群は

$e=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$, (1, 2), (1, 3), (2, 3)

(1 2 3), (1, 3, 2) とる. 下図

第1＼第2	e	(1,2)	(1,3)	(2,3)	(1,2,3)	(1,3,2)
e	e	(1,2)	(1,3)	(2,3)	(1,2,3)	(1,3,2)
(1,2)	(1,2)	e	(1,2,3)	(1,3;2)	(1,3)	(2,3)
(1,3)	(1,3)	(1,3,2)	e	(1,2,3)	(2,3)	(1,2)
(2,3)	(2,3)	(1,2,3)	(1,3,2)	e	(1,2)	(1,3)
(1,2,3)	(1,2,3)	(2,3)	(1,2)	(1,3)	(1,3,2)	e
(1,3,2)	(1,3,2)	(1,3)	(2,3)	(1,2)	e	(1,2,3)

連乗

◦ 連乗

(1) $\prod_{\mu=1}^{m} a_\mu \cdot \prod_{\nu=1}^{n} a_{m+\nu} = \prod_{\nu=1}^{m+n} a_\nu$

注) $\prod_{\mu=1}^{n} a_\mu$ の定義は $\prod_{1}^{1} a_\mu = a_1$, $\prod_{\mu}^{n+1} a_\mu = \left(\prod_{\mu}^{n} a_\mu\right) a_{n+1}$

累乗

◦ 累乗 $a=a_1=a_2=\cdots=a_n$ とした連乗

即ち $a^n=\prod_{1}^{n} a$

(1) よりただ次に

(2) $a^m \cdot a^m = a^{n+m}$

(3) $(a^m)^m = a^{nm}$ （帰納法）

第2章第6節

ここに述べた定理 (1), (2), (3) は群でない集合 即ち, 結合法則を満たすすべての集合に対して成り立つ。

○ アーベル群(可換群)に於ける連乗

定理 : アーベル群に於ける連乗の値はその因数の順序によらない。

[証明]

φ を自然数の切片 $(1, n)$ をそれ自身の上に1対1に対応させる写像とする。

$$\prod_{\nu=1}^{n} a_{\varphi(\nu)} = \prod_{\nu=1}^{n} a_\nu$$

を証明すればよい。 $n=1$ の時は明らかに成り立つ。

この主張が $n=m-1$ の時正しいと仮定する。 $n=m$ とし m に写像させられる原像を k とする。(即ち, $\varphi(k)=m$)

$$\prod_{\mu=1}^{m} a_{\varphi(\mu)} = \prod_{\mu=1}^{k-1} a_{\varphi(\nu)} \cdot a_n \cdot \prod_{k+1}^{m} a_{\varphi(\mu)} = \prod_{\mu=1}^{k-1} a_{\varphi(\mu)} \cdot \prod_{\mu=1}^{m-k} a_{\varphi(k+\mu)} \cdot a_m$$

ここで 切片 $(1, m-1)$ をそれ自身へ写す写像 φ を

$$\varphi(\mu) = \varphi(\mu) \qquad (\mu < k)$$
$$\varphi(\nu) = \varphi(\mu+1) \qquad (\mu \geq k)$$

とすると。

$$\prod_{1}^{m} a_{\varphi(\mu)} = \prod_{1}^{k-1} a_{\varphi(\mu)} \prod_{1}^{m-k} a_{\varphi(k-1+\mu)} \cdot a_m = \prod_{1}^{n-1} a_{\varphi(\mu)} \cdot a_m$$

帰納法の仮定より.

$$\prod_{1}^{m} a_{\varphi(\mu)} = \prod_{1}^{m-1} a_{\varphi(\mu)} \cdot a_m = \prod_{1}^{m-1} a_\mu \cdot a_m = \prod_{1}^{m} a_\mu$$

注1. 上の事実からアーベル群では $\prod_{1 \leq i < k \leq n} a_{ik}$ とか $\prod_{i<k} a_{ik}$ $(i=1, \cdots, n,\ k=1, \cdots, n)$ のような書き方をしてもよい。

なお a の0乗を1, a^{-m} を $(a^{-1})^n$ によって定義する (規則2, 3は成立)

注2 加群に於いては $\prod$ の代わりに $\sum$ を用いる。この時 演算規則 (3) は結合法則の形となる。 $n \cdot ma = nm \cdot a$ 規則 (2) の方は 分配法則の形となる。

分配法則

$ma + na = (m+n)a$

注3 注2によって得られた分配法則の形の他に $m(a+b) = ma + mb$ が考えられる。(乗法的には $(ab)^m = a^m b^m$) しかしこれはアーベル群にしか成り立たない。

アーベル群の時は

$m=1$ の時成立 $m=n$ の時成り立つと仮定すれば

$(n+1)(a+b) = n(a+b) + (a+b) = na + nb + a + b = (n+1)a + (n+1)b$

よって m が正整数の時は証明された $m=0$ についても主張は明白

m が負整数の時は負の累乗（累加）の定義を用いて，m が正の場合に帰着

Sn 3 アーベル群に於いて

$$\prod_{\nu=1}^{n}\prod_{\mu=1}^{m} a_{\mu\nu} = \prod_{\mu=1}^{m}\prod_{\nu=1}^{n} a_{\mu\nu}$$

が成り立つ

［証明］

$\prod_{\alpha=1}^{k} a_\alpha$ は k が有限な時その順序によらない（前項定理）n, m はもちろん有限である。第4節 Sn. 3 からわかる様に $a_{\mu\nu}$ は有限である。又任意の μ, ν をとってできた $a_{\mu\nu}$ は明らかに $a_{\mu\nu}$ に含まれる又この逆もいえる。よって両辺の積は因数の順序がちがうだけである。

Sn 4 アーベル群に於いて

$$\prod_{\nu=1}^{n}\prod_{\mu=1}^{\nu} a_{\mu\nu} = \prod_{\mu=1}^{n}\prod_{\nu=\mu}^{n} a_{\mu\nu}$$

が成り立つ

［証明］ $n=1$ の時は $\nu=1$，$\mu=1$ になるから定理は明白，$n=m$ の時成り立つとすると

$$\prod_{\nu=1}^{m+1}\prod_{\mu=1}^{\nu} a_{\mu\nu} = \prod_{\nu=1}^{m}\prod_{\mu=1}^{\nu} a_{\mu\nu} \cdot \prod_{\mu=1}^{m+1} a_{\mu(m+1)}$$

$$\prod_{\mu=1}^{m+1}\prod_{\nu=\mu}^{m+1} a_{\mu\nu} = \prod_{\mu=1}^{m+1}\left(\prod_{\nu=\mu}^{m} a_{\mu\nu}\cdot a_{\mu(m+1)}\right)$$

$$= \prod_{\mu=1}^{m}\left(\prod_{\nu=\mu}^{m} a_{\mu\nu}\cdot a_{\mu(m+1)}\right)\cdot a_{(m+1)(m+1)}$$

$$\overset{*}{=}\left(\prod_{\mu=1}^{m}\prod_{\nu=\mu}^{m} a_{\mu\nu}\cdot \prod_{\mu=1}^{m} a_{\mu(m+1)}\right)\cdot a_{(m+1)(m+1)}$$

$$= \prod_{\mu=1}^{m}\prod_{\nu=\mu}^{m} a_{\mu\nu}\cdot \prod_{\mu=1}^{m} a_{\mu(m+1)}$$ （$*$ はその因数がそれぞれ等しい）

Sn 5 対称群 S_n の位数は，$n! = \prod_{1}^{n}\nu$ である

［証明］ $n=1$ の時は明白 $n=m$ の時成り立つとする。$n=m+1$ の時はまず1の置換の数（1, 2, ⋯, $m+1$）によって対称群を分ける。（例えば $1\to 1$ なる置換を含む置換全体を S'_{m+1} 等と書く）そのそれぞれの位数は $m!$ で，分けた個数が $m+1$ 個であるから Sn 3（第4節）によりその位数は $(m+1)!$ である。

第2章第7節

§7 部分群

部分群

○ 部分群（H）

1. Hが2つの要素を含めば，積 ab をも含む
2. Hが要素 a を含めば，逆要素 a^{-1} をも含む

（ H ⊆ 郡 G ）

注） 1, 2の代わりに 〈Hが a, b を含めば ab^{-1} をも含む〉をとってもよい。
加法の群では 〈Hが a, b を含めば $a-b$ をも含む〉をとる。

○ 部分群の例

1. 単位群 E （群Gの単位要素のみからなる群）
2. 交代群 A_n （対称群 S_n のうち差積 $\Delta=\prod_{i<k}(x_i-x_k)$ の値を変えないようなもの）

生成される

○ 生成される群 … 群Gの要素 $a, b, \cdots$ を含む群全体の共通集合
$a, b, c, \cdots$ から生成される群はこのうちの有限個から作られるすべての積からなる。

巡回群

○ ただ1つの要素 a から生成される群 …… 累乗 $a^{\pm m}$（$a^0=e$ も含む）全体から成る
又これはアーベル群である。この群を 巡回群という。

▷ 巡回群
- 位数が有限である （$h\neq 0$ で $a^h=e$ となる h が存在する）
- 位数が無限である （$h=0$ でしか $a^h=e$ とならない）

位数

注） この時 巡回群（a によって生成される）の位数をこの要素 a の群Gに対する位数という。又 a の位数が h なら $a^k=e$ を満たす最小自然数は h に等しい。

Sn 1.

○ アーベル群に於て位数 m の要素 a と位数 n の要素 b との積 ab の位数は $(n, m)=1$ の時 mn である。

[証明] ab の位数を k とする $(ab)^k=e$ ∴ $a^k=b^{-k}$
両辺を m 乗すると $a^{mk}=b^{-km}$ $a^{mk}=e$ ∴ $b^{-km}=e$
ところが b の位数は n だから $n \mid km$ $(n, m)=1$ より k は n の倍数である。又 $a^{mk}=b^{-km}=e$ より同様にして k は m の倍数 ∴ k は $[n, m]$ 即ち mn の倍数 ところが $(ab)^{mn}=a^{mn}b^{mn}=e$ より k は mn である。

注） $a^h=e$ なる h が存在すれば h は a の位数 m の倍数であることは容易に証明される。（∵ $h=mk+r$ として a^r が e となることより $r=0$ である 又このような m が位数であることは $a, a^2, \cdots, a^m$ と並べてみれ

容易に想像がつく）

Sn2 ◦ $n-1$ 個の互換 $(12), (13), \cdots, (1n)$ は対称群 S_n を生成する。$(n>1)$

［証明］ $n=2$ の時 対称群 S_2 は e と (12) のみから成るから (12) 及び $(12)^2$ でまに合う。S_{n-1} の時も定理が成り立つとする。S_n の任意の置換 σ に対して n に写像される要素を i とするまず $(1n)$ を行い $(1i)$ を行なうと $i \to n$ が行われたことになる。後は $1 \sim n-1$ の数の置換でよいから定理は成り立つ。

Sn3 ◦ $n-2$ 個の3項巡回置換 $(123), \cdots\cdots, (12n)$ は交代群 A_n を生成する $(n>2)$

［証明］ 差積 Δ は互換の度に符号を変えるからすべての置換 σ は上の Sn2 より $(1i)$ の積の形にした時その数が偶数か奇数どちらかに一定する。交代群 A_n は明らかにこの中で偶数個の因数をもつものである。今 $(12i)$ で生成される群が偶置換であることは

$$(12\ i) = (1\ i)(12)(1\ i)(12)$$

であることから容易にわかる。σ を任意の偶置換とせば

$$\sigma = \prod_{s=1}^{2m} (1\ a_s) = \prod_{r=1}^{m} (1\ a_r)(1\ b_r), \quad (a_r \neq b_r)$$

と表わせる。ところが

$a_r, b_r \neq 2$ ならば

$$(1\ a_r)(1\ b_r) = (12\ a_r)^2 (12\ b_r)$$

a_r, b_r の一方どちらかが2ならば（$a_r = 2$ とする）

$$(1\ 2)(1\ b_r) = (12\ b_r)$$

即ちいずれの場合（e はもちろん $(12i)^3$ で属する）でも偶置換は $(12i)$ の積で表わされる。よって A_n は $(12i)$, $(i=3, \cdots, n)$ によって生成される。

部分群 ◦ 巡回群の部分群は単位要素 (e) のみからなるか，（部分群 H の中で）最小正指数 m をもつ要素 a^m の累乗からなる。後者は即ち H はもとの群の各要素を m 乗したものからなる。もとの群 G が無限位数の時は m は任意であるが有限位数 n の時は m は n の約数で H の位数は n/m である。逆にこのような m には巡回群 $\{a\}$ の1つ（ただ1つ）の部分群 $\{a^m\}$ が対応する。（証明略）

第2章 第8節

§8 群の部分集合の演算，剰余類

部分集合の積

◦ 群Gの部分集合の積とは　H, KをGの部分集合とする時

$h \in H \qquad k \in K$

なるh, kの積 hkの集合である。これを　HK と書く。

部分群の積

◦ H, KをGの部分群とする時

$HH = H \quad , \quad KK = K$

(即ち $a \in H, b \in H$ なるば $ab \in H$ ということ)

◦ HKの要素 hkの逆要素は $k^{-1}h^{-1}$ であるがこれは明らかに KHの要素である。HKが群になるためにはこれより $HK = KH$ でなければならない。又 $HK = KH$ だと $(HK)(HK) = HKHK = HH \cdot KK = HK$ 故に $HK = KH$ は HKが群になるための必要十分条件である。

注)　$HK = KH$ は可換群の部分群では容易に成り立つ，しかし非可換の群の時にも成り立つこともあり，この性質は群Gの可換性とは直接関係しない。

積を加法的に書く時はこの時は $H+K$ とせずに (H, K) と書く。

▷ 剰余類

剰余類

Hを群Gの部分群とする時，$a \in G$ に対して

左剰余類　aH
右剰余類　Hb

(aH は $h \in H$ なるhとaの積 ahのつくる集合とする。)

◦ 異なる剰余類は要素を共有しない

[証明]　$ah_1 = bh_2$ とすると

$h_1 h_2^{-1} = a^{-1}b$ 故に $a^{-1}b$ は Hに含まれる。ところが

$bH = aa^{-1}bH = a(a^{-1}b)H = aH$

注) この証明では $h \in H$ の時 $hH = H$ を使っている。

◦ どの要素 a ($\in G$) も1つの剰余数 aHに属す。($\because e \in H$)

▷ 群Gは部分群 Hの剰余類によって類別される。群Gの要素はすべてただ1つの剰余類に属している。どの剰余類も対等である。

○ 剰余類には $a \in H$ に対して $aH = H$ だから H 自身が含まれている。又単位要素 e をもつのは H だけだから H の他の剰余類は群にならない。

指数

○ 剰余類の個数（無限の場合も入れて）を H の G に対する指数という。G の位数（有限として）を N，H の位数を n，H の G に対する指数を f とすれば

$$N = nf$$

（注 G を無限とに濃度の計算を導入すればこの式は成り立つ

○ H を a によって生成される巡回群とする時 G の位数（有限として）は H の位数の倍数であるから G の位数を n とすれば

$$a^n = e$$

が成り立つ。

○ すべての左剰余類が同時に右剰余類になる場合がある この時

$$aH = Ha \qquad (a \in G)$$

である。このような部分群 H 即ち G のすべての要素 a と可換な部分群 H のことを，G の正規部分群又は不変部分群とよぶ。

正規部分群
不変部分群

H が正規部分群ならば剰余類の積が又剰余類になる。

$$(aH)(bH) = aHbH = abHH = abH$$

Sn. 1

○ S_3 の各部分群について右剰余類，左剰余類を求める。

S_3 ; (1 2), (1 3), (1 2 3), (1 3 2), e
(2 3)

部分群 ＼ 要素	e		(1 2)		(1 3)		(1 2 3)		(1 3 2)		(2 3)	
(1 2), e	H_0	K_0	H_0	K_0	H_1	K_1	H_2	K_1	H_1	K_2	H_2	K_2
(1 3), e	H_0	K_0	H_1	K_1	H_0	K_0	H_1	K_2	H_2	K_1	H_2	K_2
(2 3), e	H_0	K_0	H_1	K_1	H_2	K_2	H_2	K_1	H_1	K_2	H_0	K_0
(123),(132), e	H_0	K_0	H_1	K_1	H_1	K_1	H_0	K_0	H_0	K_0	H_1	K_1

この表から S_3 の正規部分群は交代群 A_3 一つであることがわかる。

Sn. 2

○ どんな部分群についてもひとつの左剰余類の要素の逆要素全体は，右剰余類を作る。部分群 H の G に対する指数は左右どちらの剰余類で考えても等しい。

［証明］ aH の一つの要素 ah の逆要素は $h^{-1}a^{-1}$ である。

$h^{-1} \in H$ であるからこれらは右剰余類 Ha^{-1} を作る。同様に Ha^{-1} からもその逆要素が aH となり aH と Ha^{-1} は対等である 従って aH と Ha^{-1} は同じ位数をもつ 上述の指数と位数の関係から後者は容易。

第2章 第8節

Sn.3 ◦ 指数2の部分群は必ず正規部分群である。対称群 S_n 中の交代群 A_n は正規部分群である。

［証明］ 指数が2であるから右剰余類は H, aH の2つである。

但し $H \neq aH$ としておく。Gのすべての要素は H か aH に属するから、部分群 H に属さない群Gの要素はすべて剰余類 aH に属する。

左剰余類についても同様で H に属さないGの要素全体が H 以外の剰余類に属する。このようなHに属さない要素 a の作る剰余類は aH と Ha で表わされるから このような a に対して $aH = Ha$ である。

又 H に属す要素 b について $bH = H = Hb$ は明らか。

対称群の場合 S_n の位数は $n!$ A_n の位数は $n!/2$ であるから A_n の S_n に対する指数は2で先の証明より A_n は正規部分群である。

Sn.4 ◦ アーベル群の部分群は必ず正規部分群である。

［証明］ $ah \in aH \longrightarrow ah = ha \longrightarrow ah \in Ha$

aH の要素 α は同時に Ha の要素 逆も成り立つ 故に $aH = Ha$

Sn.5 ◦ Gの要素で、Gのすべての要素と可換なものは、この群の中で正規部分群 Z_n を作る。（群の中心）

群の中心

［証明］ このような要素の集合を H とする H が群なら正規部分群であることは明らか。H が群であることを示す。H は e を含む。（$\because ae = ea = a$）

H が a を含めば a^{-1} をも含む

$\because$ 任意の要素 c に対して $ac = ca$ 左右から a^{-1} を乗じて

$ca^{-1} = a^{-1}c$, a^{-1} も又すべての要素と可換である。

H が a, b を含めば ab をも含む

$\because c(ab) = (ca)b = (ac)b = a(cb) = (ab)c$

よって H は群 即ち正規部分群である。

Sn.6 ◦ Gは a によって生成される巡回群とし、H は E と異なる部分群、m は a^m の H に含まれる最小指数とする。この時 $1, a, a^2, \cdots, a^{m-1}$ が H の剰余類の代表で、m は H の G に対する指数である。

［証明］ H の要素は a^{mp} の形である。今 a^s, a^t の s, t の差が m の倍数とするこの時 $s - t = mg$ a^s の属する剰余類 a^sH は a^{mp+s} なる形全体である。又 a^t の作る剰余類は $a^{mr+t} = a^{mr'+s}$ となり従って a^s と a^t は同じ剰余類に属する。

又 a^s, a^t が同じ剰余類に属す時は $a^{mp+s} = a^{mr+t}$ でGの位数が0でも n でも s と t の差は m の倍数である。

従がって剰余類の代表とには普通の整数の剰余類をとればよい。

Sm.7 ◦ H の G における どの2つの剰余類をとっても，その積が又左剰余類になるならば H は G の正規部分群である。

［証明］ H の任意の剰余類を aH, bH とする。

積 $(Ha)(Hb)$ は要素 h_1ah_2b $(h_1, h_2 \in H)$ 全体からなっている。

これが 剰余類 Hc に常に属しているから $h_1ah_2b = h_3c$ なる c が a, b に対して h_3 が h_1, a, b, c, h_2 に対して定まる。

両辺に左から h_1^{-1}，右から b^{-1} を乗じて

$$ah_2 = h_1^{-1}h_3cb^{-1}$$

$h_1^{-1}h_3 \in H$ であるから $aH = Hcb^{-1}$, $aH = Hd$, $(d = cb^{-1})$

即ち任意の左剰余類がある右剰余類と全く一致する。

要素 a は Ha に属すのであるから $Hd = Ha$ で よって $aH = Ha$

同型 自己同型

§9 同型，自己同型

▷ 同型 2つの集合 $M, \overline{M}$ に1対1対応がつき M の要素間の《関係》をその対応によってくずさずに $\overline{M}$ に写される時 2つの集合は 同型であるといい $M \fallingdotseq \overline{M}$ と表わす。この対応を同型対応という。

群の同型 ◦ 群の同型 とは2つの群 $M, \overline{M}$ との上の対応によってくずされない関係が群の積であるものをいう。

（即ち $a \to \overline{a}$, $b \to \overline{b}$ ならば $\overline{a}\,\overline{b} \to \overline{ab}$ ）

◦ 群の同型対応により単位要素は単位要素に逆要素に，部分群は部分群に写される。

［証明］ $ea = a$ であるから $\overline{e}\,\overline{a} = \overline{a}$ 即ち M の単位要素は $\overline{M}$ の単位要素に写される。

$aa^{-1} = e$ であるから $\overline{a}\,\overline{a^{-1}} = \overline{e}$ 即ち M の逆要素は $\overline{M}$ の逆要素に写される。

$HH = H$, $h_1h_2 = h_3$, $\overline{h_1}\,\overline{h_2} = \overline{h_3}$

故に $\overline{H}\,\overline{H} = \overline{H}$, $hh^{-1} = e$ $\overline{h}\,\overline{h^{-1}} = \overline{e}$, $\overline{h}^{-1} \in \overline{H}$

よって 部分群は部分群へ写される。

◦ 以下 同型な群は皆同じものとみなし区別しない。

注） 同型な群では一方に成り立つ定理は同型対応によって他方にそっくりそのまま移される。

◦ 特に 集合 M と $\overline{M}$ が同一の時この同型を自己同型という。自己同型対応には恒等対応 e が含まれる σ, τ が含まれる時変換の積 $\sigma\tau$ も又含ま

第2章第9節

同型
自己同型群

又 σ^{-1} も又含まれる。よって自己同型の集合は群をつくる。この群を自己同型群という。群 G の自己同型はまた群 A(G) になる。

▷ 群の自己同型 { 内部自己同型 … $\bar{x} = axa^{-1}$ $(a \in G)$
　　外部自己同型 … 上以外の自己同型

対応 $\bar{x} = axa^{-1}$ が自己同型であるのは次からわかる。

$x = a^{-1}\bar{x}a$ （1対1対応）

$\bar{x} = axa^{-1}$, $\bar{y} = aya^{-1}$ ならば

$\bar{x}\bar{y} = axa^{-1} \cdot aya^{-1} = axya^{-1} = \overline{xy}$

- axa^{-1} を x を a によって変換した要素といい，x に共役な要素ともいう。aHa^{-1} に対しても同様。
- 群 G の部分群 H が任意の内部自己同型に対して不変な時 H は正規部分群（不変部分群）である。

$$aHa^{-1} = H$$

より

$$aH = Ha$$

即ち H は正規部分群である。

注） $aHa^{-1} = H$ の代わりに $aHa^{-1} \subseteq H$ でも H は正規部分群となる。（∵ aHa^{-1} の a を a^{-1} とかえて $a^{-1}Ha \subseteq H$ これと前から $aHa^{-1} = H$）

Sn. 1

- アーベル群に於ては恒等自己同型以外，内部自己同型は存在しない。4つの要素 e, a, b, c から成り e を単位要素とし結合関係 $a^2 = b^2 = c^2 = e$, $ab = ba = c$, $bc = cb = a$, $ca = ac = b$ をもつ群では恒等自己同型以外内部自己同型はないが5個の外部自己同型をもつ。

［証明］ アーベル群では $\bar{x} = axa^{-1} = aa^{-1}x = x$ 即ちすべての内部自己同型は恒等自己同型となる。

$\bar{e} = e$ だから $\bar{a}$ は a, b, c のうちのいずれかである。

$\bar{a} = a$ とすると恒等自己同型は省いておくのだから $(b\ c)$ である。

$\bar{a} = b$ とすると $\bar{b} = c$ と $\bar{b} = a$ の2通りになりそれぞれ (ab) と $(a\ b\ c)$ になる。 $\bar{a} = c$ からも同様にして $(a\ c), (a\ c\ b)$

故に $(ab),(bc),(ac),(abc),(acb)$ の外部自己同型が存在する。この自己同型群は 3次の対称群である。

Sn. 2 ◦ 置換群に於て，要素 b を要素 a で変換するには，b を 巡回 置換の積で表わし。この巡回 置換内の数字に a の置換をほどこせばよい。又これを用いて $b=(12)(345)$，$a=(2345)$ の時に aba^{-1} を計算する。

[証明] b が1個の巡回置換 $(i_1 \cdots i_r)$ で表わされる時，

$a(i_1 \cdots i_r)a^{-1}$ は最初 $a(i_k)$ なる要素が次に i_k となり次に i_{k+1} になり次に $a(i_{k+1})$ 即ち $a(i_k) \to a(i_{k+1})$ である。従って

$a(i_1 \cdots i_r)a^{-1} = (a(i_1)\ a(i_2)\ \cdots\ a(i_r))$ である。

次に b が s 個の巡回置換で表わされる時定理は成り立つと仮定する。 b が s+1 個の巡回置換で表わされる時

$b = (i_1 \cdots i_r)b'$ （b' は s 個の巡回置換の積）

とすると

$$aba^{-1} = a(i_1 \cdots i_r)b'a^{-1}$$
$$= a(i_1 \cdots i_r)a^{-1} \cdot ab'a^{-1}$$
$$= (a(i_1)\ a(i_2) \cdots a(i_m))\ ab'a^{-1}$$

となり b' の巡回置換については定理は成り立つからすべての b について定理は証明された。（証明終）

次に後者の計算をする

$$aba^{-1} = (a(1), a(2))(a(3)\ a(4)\ a(5))$$
$$= (13)(452)$$

Sn. 3 ◦ 対称群 S_3 には外部自己同型はなく，6個の内部自己同型がある。

[証明] Sn 2 と同じ考え方で $(a(i_1)\ a(i_2) \cdots a(i_r))$ が $a(i_1 \cdots i_r)a^{-1}$ となることが容易にわかる。

S_3 の要素は $(12),(13),(23),(123),(132),e$ であるが自己同型対応によって互換は3項の巡回置換に移らない逆も同様（∵ a を互換とすれば $a^2=e$ ∴ $\bar{a}^2=e$）

1. $(12) \to (12)$
   - $(13) \to (13)$ …… 恒等自己同型
   - $(13) \to (23)$ …… $a=(12)$ とすれば
     $a(12)a^{-1}=(12)$，$a(13)a^{-1}=(23)$，
2. $(12) \to (13)$
   - $(13) \to (12)$ $a=(23)$ ととれる $(12)=(a(1)\ a(2))$

第2章第9節

S_n 3

$\circ\ (13) \to (23)$ $\quad a=(132)$

3 $(12) \to (23)$

$\circ\ (13) \to (12)$ $\quad a=(123)$

$\circ\ (13) \to (13)$ $\quad a=(13)$

以上の6個の内部自己同型がある。

S_n 4

$\circ$ 対称群 S_4 は，それ自身と単位群の外に，次の正規部分群をもつにすぎる!!。

a) 交代群 A_4

クラインの四元群

b) クラインの四元群 V_4

$1,\ (12)(34),\ (13)(24),\ (14)(23)$

[証明]

S_4 の置換群を次の4つの型に分ける。

①(ij)，②(ijk)，③$(ij)(kl)$，④$(ijkl)$

ここで $i\ j\ k$ 等は常に1234の中の1つを表わしどれも等しくない!!とする（このような分け方は常に可能である）

ここでそれぞれに σ によって変換を加えると

① $(ij) \to (i^\sigma j^\sigma)$ ② $(ijk) \to (i^\sigma j^\sigma k^\sigma)$

③ $(ij)(kl) \to (i^\sigma j^\sigma)(k^\sigma l^\sigma)$ ④ $(ijkl) \to (i^\sigma j^\sigma k^\sigma l^\sigma)$

ここで $\sigma H \sigma^{-1} = H$ であるからこのそれぞれも又Hに属さなければならない!!。もしHが(ij)を要素に含んだとするとそれは①の変換よりすべての互換を含む S_4 は互換によって生成されるからHは S_3 自身となる。次にHが(ijk)を含んだとするとすべての三項巡回置換(ijk)を含むことになる。これらの積からは交代群 A_4 ができるが。A_4 の位数は12であるから部分群の位数が24の約数であることを考えれば A_4 を含む部分群は S_4 以外になく。交代群A_4以外(ijk)を含むことはない!!。次にHが$(ij)(kl)$を含んだとする。これには③の変換から任意の$(ij)(kl)$を含む又これだけで群をつくるからこれも一つの正規部分群 V_4 である。次にHが$(ijkl)$を含んだとするこの時$(ijkl)$は奇置換であるからこれだけでは群をつくらない!!従ってHが群をつくるためには③と④の形を含まなければならない!!。③と④のすべてを含むことは前と同じであるからHは$(ijkl)$と$(ik)(jl)$を含むこれらの積は(jl)となってHが互換を含むことになる3従ってHは S_4 自身となる。よって S_4 の正規部分群は A_4 と V_4 だけである。

Sn. 5 ◦ N を G の正規部分群とし，H を N と G の中間にある群とする

$$N \subseteq H \subseteq G$$

すると，N は H の正規部分群である。

[証明] H の要素 a に対して $aH = Ha$ が成り立つから N は H の正規部分群である。（$\because a \in G$）

Sn. 6 ◦ 無限巡回群は整数の加群 Z に同型である。

[証明] 無限巡回群 $\{a\}$ の要素 a^m に対して整数 m を対応させる。この時 $\overline{a^m} = m$，$\overline{a^n} = n$ である。

積 $a^m \cdot a^n = a^{m+n}$ に対しては $\overline{a^{m+n}} = m+n = p$

和 $m + n = p$，が対応する。（証明終）

Sn. 7 ◦ 群 G で，1つの要素 a と可換な要素 x は G の部分群をなす。

正規化群 これを，a の正規化群 $N(a)$ という。この群は a によって生成される巡回群を正規部分群として含んでいる。a に共役な要素の個数は，a の正規化群の G に対する指数に等しい。

[証明] $x \in N(a)$ に対して $ax = xa$ であるから x^{-1} を左右からかけて $x^{-1}a = ax^{-1}$ 故に $x^{-1} \in N(a)$，$ea = ae$ であるから。$e \in N(a)$ $ax = xa$，$ay = ya$ ならば 即ち $x \in N(a)$ $y \in N(a)$ ならば $axy = xay = xya$ 故に $xy \in N(a)$ よって $N(a)$ は群である。次に $a^m \cdot a = a \cdot a^m$ であるから $\{a\} \subseteq N(a)$ がわかる。$N(a)$ の要素 x に対して $xa^m = a^m x$ であるから $\{a\}$ は $N(a)$ の正規部分群である。次に $N(a)$ の剰余類を $N(a)$，$b_i N(a)$，…，$b_r N(a)$，と書く但しどの2つも同じ要素を共有しない。同じ剰余類に属する要素 $b_i x$，$b_i y$ の変換を a に加えると $b_i x\, a\, x^{-1} b_i^{-1} = b_i\, a\, b_i^{-1} = b_i y\, a\, y^{-1} b_i^{-1}$ となってすべて等しくなる。又ちがった剰余類に属する要素 $b_i x$，$b_j y$ の変換を a に加えるとそれぞれ $b_i\, a\, b_i^{-1}$，$b_j\, a\, b_j^{-1}$ となる。この2つは相異なる。なぜなら $b_i\, a\, b_i^{-1} = b_j\, a\, b_j^{-1}$ だと両辺に左右から b_j^{-1}，b_i を乗じて $b_j^{-1} b_i\, a = a\, b_j^{-1} b_i$ よって $b_j^{-1} b_i$ が $N(a)$ に属する。$b_j^{-1} b_i = x$ なる $N(a)$ の要素 x が存在する。左から両辺に b_j を乗じると $b_i = b_j x$ となる。b_i は明らかに $b_i N(a)$ に属する。ところが $b_j x$ は明らかに $b_j N(a)$ に属する。従ってこの2つの剰余類が同じ要素を共通することになり，仮定に反する。従って $b_i\, a\, b_i^{-1} \neq b_j\, a\, b_j^{-1}$ で $b_i N(a)$ と $b_i\, a\, b_i^{-1}$ の対応を考えると1対1対応となる。よって 剰余類の G に対する指数は a に共役な要素の個数に一致する。

第2章第9節

Sn. 8

◦群Gの要素を互いに共役な要素の類に分けることができる。Gが有限群の場合は1つの共役類の要素の個数はGの位数の約数である。単位要素も、中心の要素も、それ1個だけで共役類をなす。

[証明] 群Gの任意の要素aをとりそれと共役な要素 xax^{-1} をすべてあげる。この時 $b=xax^{-1}$, $c=yay^{-1}$ であるb, cについて $yx^{-1}bxy^{-1}=c$ であるからbとcも共役である。次にaと共役でない要素bをとる。aと同様にしてbと共役なものをすべてあげる。この時aに共役なものとbに共役なものが一致することはない。なぜなら $b=xax^{-1}$ るるxは仮定により存在しるが、aのある共役要素 $\bar{a}=uau^{-1}$ とbのある共役要素 $\bar{b}=vbv^{-1}$ が等しいるら $uau^{-1}=vbv^{-1}$ より $v^{-1}uau^{-1}v=b$ となり仮定に反す。よってaの共役類とbの共役類は要素を共有しる。同様にしてそれ以外の要素cも考える。こうしてGの各要素の作る共役類は互いに全く一致するか一つも要素を共有しるかのいずれかである。即ちGの要素aを一つ定めればそれによってただ一つの共役類を決定しaをその中に含まれるようにすることができる。そして上述よりどの共役類も要素を共有しる。よって群Gの各要素を互いに共役な要素の類に分けることができる。Gが有限群るら Sn 7 よりそれはGの正規化群の指数に等しいからGの位数の約数である。単位、要素、中心の要素は共にGのすべての要素と可換だから明らかにその共役類はそれ自身からる。

Sn 9

◦pを素数とする時、位数 p^m の群Gに於て要素の個数 p^λ の共役類が a_λ 個あるとし特に中心の要素は a_0 個あるとする。そうすると等式（類方程式という）

類方程式

$$p^m = a_0 + a_1 p + a_2 p^2 + \cdots$$

が成り立つ。この等式から位数 p^m の群の中心が単位要素と異なる要素を必ず含むことがわかる。（位数 p^m の群を、P－群と呼ぶ）

P－群

[証明] 等式は群Gの要素を共役類別に加えたことによる。又Pが素数（$p\geq 2$）であることから a_0 はPの倍数で正であるから少なくてもPである。よって $p\geq 2$ より定理が成り立つ。

注) Sn. 7でGを有限群としなかったのは証明中用いられた等しい概念が1対1に対応するということであってこれは無限群の場合の濃度の計算に適応できる。従って個数が等しいという代わりに濃度が等しいといえば明確になる。Sn 8では約数ということから Sn 9 への準備としてGを有限群と限った。

§10 準同型，正規部分群，剰余群

準同型 ▷ **準同型**

1. $\bar{M}$ のどの要素 $\bar{a}$ も，M の少なくても1つの要素 a の像となる。
2. M の要素の間に成り立つすべての関係は，$\bar{M}$ の対応する要素間にも成り立つ。

$\bar{M}$ … “準同型な像”

重複同型 注） 準同型のことを 重複同型ともいう。

- “M が $\bar{M}$ に準同型である” の記号 …… $M \sim \bar{M}$

  （正確には M が $\bar{M}$ に準同型に写像しえる時 … $M \sim \bar{M}$）

自己準同型 ・自己準同型 …… $M \sim \bar{M}$ の時 $\bar{M} \subseteq M$ なる場合

単純同型 ・単純同型 …… $M \sim \bar{M}$ で $\bar{M} \sim M$ なる時（＝同型）

- 準同型写像がある時 $\bar{M}$ の1つの要素 $\bar{a}$ に写像される M の要素全体を，1つの類 A にまとめることができる。このようにして類をつくると集合 M は類別され，その各類が $\bar{M}$ の要素と1対1に対応する。

▷ 群 G が 積の定義される集合 $\bar{G}$ に準同型であるとすると $\bar{G}$ も又群である。次に同型と同じことが成り立つ。 （証明略）

1. 単位要素は単位要素に写像される。
2. 逆要素は逆要素に写像される。

▷ 群 G の準同型 $G \sim \bar{G}$ に於て，$\bar{G}$ の単位要素 $\bar{e}$ に写像される G の類 N は G の正規部分群で，他の類はこの正規部分群の剰余類である。

［証明］ N が群であることは $e \to \bar{e}$ より $e \in N$，$x \to \bar{e}$ なら $x^{-1} \to (\bar{e})^{-1} = \bar{e}$ より $x \in N$ なら $x^{-1} \in N$，$x \in N$，$y \in N$ なら $xy \to \bar{x}\bar{y} = \bar{e}\bar{e} = \bar{e}$ より $xy \in N$ がいえる。又 剰余類 aN を作るとこの任意の要素は $ax \to \bar{a}\bar{x} = \bar{a}$ に写像される 逆にある要素 u が $\bar{a}$ に写像されれば $av = u$ として（除法の可能性） $u \to \bar{a}$，$a \to \bar{a}$ を作れば $v \to \bar{e}$ で $v \in N$ である。よって $u \in aN$ となり。このような u はすべて aN に属す。よって要素 $\bar{a}$ に写像される群 G の類は N の左剰余類 aN に全く一致する。右剰余類についても同様にして $\bar{a}$ に写像される類は Na に全く一致する。故に $aN = Na$

第2章第10節

▷ 剰余群

剰余群 … 群Gに対してその1つの正規部分群をとりその剰余類を作る。各々の剰余類を要素にその間の積を前の剰余類の積で定義すると正規部分群の剰余類の積はやはり剰余類となり，正規部分群自身と剰余類の積は同じ剰余類となる。又互いに逆要素を有する剰余類同士の積は正規部分群自身に属する。従ってこのような剰余類の集合は群をつくる。これを剰余群という。

$$\begin{cases} (aH)(bH) = aHbH = abH \\ (aH)H = aHH = aH. \\ H(aH) = HaH = aHH = aH \\ (aH)(a^{-1}H) = aa^{-1}HH = H \end{cases}$$

群Gの要素aが属する剰余類 aH にaの像をきめると 群Gから剰余群 へ の準同型写像ができる。剰余群の位数は元になる正規部分群のGに対する指数に等しい。

剰余群 …… G/N で表わす（N … 正規部分群）

因子群 ◦ Nを法とするGの剰余群 （ Nによる Gの因子群 ）

▷ 群の（第1）準同型定理

群の準同型定理

群Gの準同型な像 $\overline{G}$ は，剰余群 G/N に同型である。ここで，NはGの正規部分群で，$\overline{G}$ の単位要素に対応するすべての要素から成る。逆に，G は剰余群 G/N（Nは正規部分群）に準同型に写像される。

［証明］ $G \sim \overline{G}$ とすると $\overline{G}$ の要素には，Gの正規部分群Nの剰余類が1対1に対応することがわかっている。この対応が同型対応であることがいえればよい。

aN，bN の積は abN である。これらに対応するGの要素は $\overline{a}$，$\overline{b}$，$\overline{ab}$ であるが実際準同型によって

$$\overline{ab} = \overline{a}\,,\ \overline{b}$$

となるから $G/N \cong \overline{G}$ となる。

Sm. 1 ◦ すべての群Gは，自明な剰余群をもつ。それは $G/E \cong G$，$G/G \cong E$ である。

［証明］ $a \in G$ に対して $aE = Ea$ であるから Eは正規部分群で Eの位数は1であるから $G/E \cong G$ である。 $a \in G$ に対して $aG = Ga$ は明らか G/G の位数は明らかに1である。

Sn.2 ◦ 交代群を法とする対称群の剰余群 S_n/A_n は位数2の巡回群である。

［証明］ S_n/A_n の位数が2なのは明白，この単位要素を e，e とはちがう要素を a とせば $a^2=e$ である。 従がって S_n/A_n は a の巡回群となる。

Sn.3 ◦ クラインの四元群を法とする剰余群 S_4/V_4 は S_3 に同型である。

［証明］ S_4/V_4 と S_3 の位数は等しいから，S_4 から S_3 に $V_4\to e$ とする準同型が作れればよい。 S_4/V_4 は次の6つの要素から成る。

V_4，$(12)V_4$，$(13)V_4$，$(23)V_4$，$(123)V_4$，$(132)V_4$，

こうしておいて aV_4 に S_3 の置換 a を対応させればよい。（$V_4\to e$）

Sn.4 交換子群 交換子 ◦ 群 G の要素 $aba^{-1}b^{-1}$ とそれらの積は，群をなす。この群を G の交換子群 G' という。これは G の正規部分群で，これを法とする剰余群はアーベル群である。又逆に剰余群がアーベル群になるような正規部分群は，必ず交換子群を含む。（$aba^{-1}b^{-1}$ の形の要素を a，b の交換子といい $[a,b]$ で表わす a，b が可換る時，その時に限り $[a,b]=e$ で群 G の交換子群を $G'=[G,G]$ とかくことがある。）

［証明］ G' は e を含む（$\because\ eee^{-1}e^{-1}=e$） G' が $x=\prod_{\alpha=1}^{m} a_\alpha b_\alpha a_\alpha^{-1} b_\alpha^{-1}$ を含めば $x^{-1}=\prod_{\alpha=m}^{1} b_\alpha a_\alpha b_\alpha^{-1} a_\alpha^{-1}$ を含む。（$b_\alpha^{-1}a_\alpha^{-1}b_\alpha a_\alpha$ は b_α^{-1}，a_α^{-1} の交換子である） x，y が交換子の有限個の積ならば xy も又交換子の有限個の積であるから $xy\in G'$ 故に G' は群である。

次に $x\in G'$ ならば $x=\prod_{\alpha=1}^{m} a_\alpha b_\alpha a_\alpha^{-1} b_\alpha^{-1}$ であるが，$c\in G$ に対して $cxc^{-1}\in G'$ を証明する。

$$cxc^{-1}=c\left\{\prod_{\alpha=1}^{m} a_\alpha b_\alpha a_\alpha^{-1} b_\alpha^{-1}\right\}c^{-1}$$

$$=\prod_{\alpha=1}^{m} ca_\alpha b_\alpha a_\alpha^{-1} b_\alpha^{-1} c^{-1}$$

$$=\prod_{\alpha=1}^{m} ca_\alpha c^{-1}\cdot cb_\alpha c^{-1}\cdot ca_\alpha^{-1}c^{-1}\cdot cb_\alpha^{-1}c^{-1}$$

ここで $ca_\alpha c^{-1}=u_\alpha(\in G)$ $cb_\alpha c^{-1}=v_\alpha(\in G)$ とせば

$$cxc^{-1}=\prod_{\alpha=1}^{m} u_\alpha v_\alpha u_\alpha^{-1} v_\alpha^{-1}$$

故に $cxc^{-1}\in G'$ よって G' は正規部分群である。

アーベル群であることを証明する。 $abG'=baG'$ を証明すればよい。

$$abG'=baa^{-1}b^{-1}abG'$$

ところが $a^{-1}b^{-1}ab\in G'$ 故に $abG'=baG'$

第2章 第10節

Sn 4

逆にHを剰余群がアーベル群であるGの正規部分群とする。この時a, bの属する剰余類 aH, bHの積は abH であるこれがアーベル群であるから baHにも等しい。ところが ab = baa⁻¹b⁻¹ab であるから $h_1 \in H$, $h_2 \in H$ とすれば $abh_1 = bah_2$ だがこれから ba a⁻¹b⁻¹ab $h_1 = bah_2$ 左から a⁻¹b⁻¹ を乗じて a⁻¹b⁻¹ab $h_1 = h_2$ 右から h_1^{-1} を乗じて a⁻¹b⁻¹ab $= h_2 h_1^{-1}$ 即ち Hは任意の要素 a⁻¹, b⁻¹ の交換子を含む。よってそれらの積も含むことになり（Hは群である）Hは必ず交換子群を含む。

Sn 5
正規化群

○ 群Gの部分群Hと可換なGの要素全体は，Hを含む部分群 N(H)を作り，HはN(H)の正規部分群となる。これをHの正規化群とよぶ N(H)のGに対する指数は，Hと共役なGの部分群の個数に等しい。（このHがGの一数aの巡回群の時 §9 Sn7 の正規化群に一致する）

［証明］ まず N(H)が群であることを証明する。 $x \in N(H)$ ならば $xH = Hx$ である。左右から両辺に x^{-1}, x^{-1} を乗じて $Hx^{-1} = x^{-1}H$ 故に $x^{-1} \in N(H)$, $x \in N(H)$, $y \in N(H)$ ならば $xyH = xHy = Hxy$ となって $xy \in N(H)$ よって N(H)は群である。 $x \in N(H)$ に対して $xH = Hx$ であるからHはN(H)の正規部分群である。次にN(H)の剰余類を各剰余類から1つ代表を選んで $uN(H)$, $vN(H)$ 等と表わす。この時 $uN(H)$ と $vN(H)$ なる形がその中にあれば $v^{-1}u$ はN(H)に属さない。（∵ $v^{-1}u \in N(H)$ だと $u \in vN(H)$，一方 $u \in uN(H)$ は明白だから $uN(H)$ と $vN(H)$ が無縁であることに反す）剰余類 $uN(H)$ に属す要素 $\alpha = u\alpha$，($\alpha \in N(H)$) に対して変換 $\alpha H \alpha^{-1}$ を作ると $\alpha H \alpha^{-1} = u\alpha H \alpha^{-1}u^{-1} = uHu^{-1}$ となり 剰余類 $uN(H)$ に対して変換 uHu^{-1} がただ1つ定まる。もしちがった剰余類 $vN(H)$ が存在して vHv^{-1} が uHu^{-1} に一致したとすると $uHu^{-1} = vHv^{-1}$ より $v^{-1}uHu^{-1}v = H$ 即ち $v^{-1}u \in N(H)$ このようなことは互いに無縁な剰余類 $uN(H)$ と $vN(H)$ に対しては成り立たないことを前に示したから結局 Hの共役部分群 uHu^{-1} には剰余群 $uN(H)$ がただ1つ対応する。よって uHu^{-1} と $uN(H)$ の対応は1-1対応で uHu^{-1} の位数と N(H)の指数は一致する。

Sn 6

○ Gが巡回群で，aはGの生成要素，Nを指数 mの部分群とするとG/Nは位数 mの巡回群である。Nの剰余類の代表として，要素 1, a, a^2, …, a^{m-1} をとることができる。

［証明］ Nの指数が mだからGの位数をmとしNの位数をkとせば $m = mk$ ∴ $m = \frac{n}{k}$ ところがNの正の最小指数も $\frac{n}{k}$ で表わせるから

m は N の正の最小指数に等しい。故に $N=\{a^m\}$ である。N の剰余類 a^sN を考える。$s=mu+r$ $(0\leqq r<u)$ とする。すると、$a^sN=a^{r+mu}N$ $=a^r a^{mu}N$, $a^{mu}\in N$ であるから $a^sN=a^rN$ となる。即ち N の剰余類は a^rN $(0\leqq r<m)$ によってすべて表わされる。次に a^rN と $a^\beta N$ $(0\leqq r<m,\ 0\leqq \beta<m,\ r\neq\beta)$ が一致しないことを示す。$a^rN=a^\beta N$ だと $a^{r-\beta}\in N$ 即ち $r-\beta=m\alpha$ となる。ところが $0\leqq r,\beta<m$ だから $|r-\beta|<m$ 即ち $r-\beta=0$, $r=\beta$ これは仮定に反す。よって $a^rN\neq a^\beta N$ となり $a^0=1, a, a^2, \cdots, a^{m-1}$ が N の剰余類の代表になりうる。

▷ アーベル群ではすべての部分群が正規部分群である。結合関係を加法的に書くと群は加群 部分群は部分加群という名称になる。

部分加群
剰余加群

G/M は M を法とする剰余加群である。

合同

○ 2つの要素 a, b が同じ剰余加群 $c+M$ に属せばその差は M に属する。この関係 a, b は M を法として合同であるといい

$$a\equiv b \pmod M \quad \text{あるいは} \quad a\equiv b \ (M)$$

で表わす。この時準同型で対応する剰余加群の要素 $\bar{a}$, $\bar{b}$ に対して

$$\bar{a}=\bar{b}$$

である。逆に $\bar{a}=\bar{b}$ ならば $a\equiv b \pmod M$ である。

注) G として自然数全体をとり、M として m の倍数全体をとると、$a-b$ が m で割りきれる時 $a\equiv b \mod m$ あるいは $a\equiv b\ (m)$ と書く 自然数全体は1を生成元にする巡回群であるから 剰余類は $0, 1, 2, \cdots, m-1$ によって代表され、剰余加群は位数 m の巡回群となる。

Sm. 7

○ 位数 m の巡回群は、必ず整数 m を法とする整数の加群 $\mathfrak{Z}$ の剰余加群と同型である。

[証明] 巡回群の要素 $1, a, \cdots, a^{m-1}$ に対して整数の加群 $\mathfrak{Z}$ の剰余加群の $M, 1+M, 2+M, \cdots, m-1+M$ を対応させればよい。

注) 与えられた準同型によって単位要素に写像される正規部分群をその準同型の核という。

第3章 環および体

§11 環

環

▷ 環 ・二つの結合関係 "$a+b$" "ab" を有する代数係
・上の結合関係に下記の諸法則を有する。

I 加法の法則
a) 結合法則 $a+(b+c)=(a+b)+c$
b) 交換法則 $a+b=b+a$
c) すべての a, b について方程式 $a+x=b$ が解ける。
(即ち加法に関してアーベル群をなす この群を環の加法群という)

II 乗法の法則
a) 結合法則 $a\cdot bc=ab\cdot c$
(乗法に関して群をなす必要がないことに注意)

III 分配法則
a) $a(b+c)=ab+ac$
b) $(b+c)a=ba+ca$

更に 次の法則が成り立つ時可換環という。

IV 乗法の交換性
b) $ab=ba$

注)・Iより環は加法に関してアーベル群をなすから前にアーベル群に対して証明されたことは環に於てもすべて成り立つ。
・なお乗法については群をなさないが 連乗の定理は結合法則の成り立つものには成立することを述べたから (P.13) 成立する。
・分配法則の延長として帰納法によって

$$(a_1+a_2+\cdots+a_m)b=a_1b+a_2b+\cdots+a_mb$$
$$a(b_1+b_2+\cdots+b_m)=ab_1+ab_2+\cdots+ab_m$$

が証明される。

零要素
・IIIから因数が零要素0なら積が0になることがわかる。

▷ 零因子 …… $ab=0$, $(b\neq 0)$ a … 左零因子
$ab=0$, $(a\neq 0)$ b … 右零因子

零因子

注) 零因子は環に0以外の要素があることを仮定して定められる。

整域 0以外の零因子のない環を整域とよぶ。

▷ 単位要素

単位要素 $\begin{cases} ea=a & \cdots e \cdots \text{左単位要素} \\ a\bar{e}=a & \cdots \bar{e} \cdots \text{右単位要素} \end{cases}$

○ 単位要素が左右に存在すれば，それらは皆1つの単位要素 e に等しい。

注) 左だけに存在し右には存在しない例もある。このような時左単位要素が皆等しいとは限らない。可換環では左右の区別がないから存在すれば左右とも e に等しい。

定理は $ex=x$, $y\bar{e}=y$ として $\bar{e}=e\bar{e}=e$ ∴ $\bar{e}=e$ から容易に得られる。 (単位要素を数1で表わすことも例い)

注) 単位要素をもつ環という時は左右両方とも持つ環のことである。

▷ 逆要素

逆要素 $\begin{cases} aa_{(r)}^{-1}=e & \cdots a_{(r)}^{-1} \cdots \text{右逆要素} \\ a_{(l)}^{-1}a=e & \cdots a_{(l)}^{-1} \cdots \text{左逆要素} \end{cases}$

○ 逆要素が左右に存在すれば それらは1つの要素 a^{-1} に一致する。この時上と同様に a を逆要素をもつという。

▷ 倍要素

倍要素 環の加法群に於て

na ($a+a+\cdots+a$, n項)

を定義すると次の法則が成り立つ

1. $na+ma=(n+m)a$ … 連乗の公式(2)を加法で (P12)
2. $n\cdot ma=nm\cdot a$ … 〃 (3)を加法で (〃)
3. $n(a+b)=na+nb$ … アーベル群の可換性，
4. $n\cdot ab=na\cdot b=a\cdot nb$ … 分配法則から。

Sm 1 ○ 数の組 (a_1, a_2) で (a_1, a_2 は有理数)

$(a_1, a_2)+(b_1, b_2)=(a_1+b_1, a_2+b_2)$

$(a_1, a_2)\cdot(b_1, b_2)=(a_1b_1, a_2b_2)$

とすると，0以外の零因子をもつ環ができる。

[証明] I の a), b), c) II の a) III a), b) IV b) がすべて成り立つからこれは可換環である。零要素は $(a_1, a_2)+(x, y)=(a_1, a_2)$ より $(0, 0)$ である。今 $(a, 0)$ と $(0, b)$ の積を考えると明らかにこれは0となるよって $(a, 0)\neq 0$ であるから $(0, b)$ は零因子 又逆に $(a, 0)$ も零因子である。

Sm 2 ○ a が左零因子でなければ等式 $ax=ay$ の両辺を a で簡約してもよい。

[証明] 両辺に $a(-y)$ を加えると $ax+a(-y)=0$,

$a(x-y)=0$ $x-y\neq 0$ ならば a は零因子だから $x-y=0$

第3章 第11節

$x-y=0$ の両辺に y を加えて $x=y$ 即ち簡約できる。

注) これより 環が整域なら $ax=ay$, で $a\neq 0$ なら常に $x=y$ とできる。

Sn.3 ◦ かってるアーベル群を加法的に書き任意の2要素の積を0と定義すれば環ができる。

[証明] この集合がIを満たすことは仮定より明らか。又II a) も明らかすべての積が0であるからIII a), b) も成り立つ よってこれは環である。

Sn.4 ◦ 左零因子は左逆要素をもたない。右零要素は右逆要素をもたない。特に0に左逆要素も右逆要素ももたない。但し環には零要素0以外の要素があるとする。(0しかない場合は0は同時に単位要素にもなり0の逆要素は0とるる<零環>)

零 環

[証明] 左零因子 u には $ua=0$, $(a\neq 0)$ なる a が存在するも u に左逆要素 $u^{(-1)}$ が存在したとすると 両辺にそれを乗じて $a=0$ となり仮定に返す。右の場合も同様。 0の場合は $0a=0$, $a0=0$, $(a\neq 0)$ であるから0は同時に左右の零因子とるるから左右どちらの逆要素も存在しない。

Sn.5 ◦ かってる可換環に於て, 2項定理

2項定理

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

が成り立つ。

[証明] $n=1$ に対しては $(a+b)^1 = a+b$ であるから定理は成り立つ

$n=m$ に対して定理が成り立つとすると

$$(a+b)^{m+1} = (a+b)^m(a+b)$$

$$= \left\{a^m + \binom{m}{1}a^{m-1}b + \cdots + b^m\right\}a + \left\{a^m + \binom{m}{1}a^{m-1}b + \cdots + b^m\right\}b$$

$$= a^{m+1} + \left\{\binom{m}{1}+1\right\}a^m b + \left\{\binom{m}{2}+\binom{m}{1}\right\}a^{m-1}b^2 + \cdots + b^{m+1}$$

$$\binom{m}{r} = \frac{m(m-1)\cdots(m-r+1)}{r!} \quad \therefore \binom{m}{r}+\binom{m}{r-1} = \frac{(m+1)\cdots(m-r+2)}{r!}$$

$$= \binom{m+1}{r}, \quad \text{よって} \quad (a+b)^{m+1} = a^{m+1} + \binom{m+1}{1}a^m b + \cdots + b^{m+1}$$

となり証明された。

Sn 6 ◦ n 個の要素から成る環に於ては任意の要素 a に対して

$$na=0$$ (前章で乗法的に証明したので証明略)

Sn 7

○ a と b が可換であれば，a は $-b$ とも nb とも，b^{-1} とも可換である。
a が b 及び c と可換ならば，a は $b+c$ 及び bc とも可換である。

[証明] $a(-b)=-ab$ であるなぜならば $a(-b)+ab=a+\{(-b)+b\}$
$=a\cdot 0=0$ であるからである。同様にて $(-b)a=-ba$ である。
よって $ab=ba$ ならば $-ab=-ba$ であるから $(-b)a=a(-b)$
即ち a と $-b$ は可換である。 $a\cdot nb=nab=nba=nb\cdot a$
即ち a と nb は可換。もし b が逆要素をもてば $ab=ba$ の両辺に左右から b^{-1} を乗じて $b^{-1}a=ab^{-1}$ 即ち a と b^{-1} は可換。 $ab=ba$
$ac=ca$ ならば $a(b+c)=ab+ac=ba+ca=(b+c)a$ よって
a と $(b+c)$ は可換。 $abc=bac=bca$ よって a と bc は可換。

体 ▷ 体

- ○ 環の条件
- ○ 下記の2条件
  - a) 0 以外の要素を少なくとも1つ含む
  - b) $a\neq 0$ に対して $\begin{cases} ax=b \\ ya=b \end{cases}$ が解を持つ。

斜体 ○ 上記の条件を有する環を斜体といい。これが可換の時 体とよぶ
（体を有理域 <英語 field> ともいう）

注）なお斜体を体と呼びその中で可換体と非可換体を区別することもある。

▷ 斜体（体）は加法的アーベル群で更に0を除く要素全体は乗法に関して群を作る。乗法に関して群を作る0以外の体の要素全体をその体の乗法群という。（従って乗法に関する前章でみた群の性質は0を除く体の要素全体に対して成り立つ）

乗法群

Sn 8

○ 斜体（体）には単位要素 e が存在する。又0以外の要素の逆要素が存在する。

[証明] 斜体の0以外の要素が乗法群をつくることから明らかであるがあるために証明する。まず $a\neq 0$ に対して $ax=a$, $ya=a$ を解くとその解は両方とも等しく e とする。この時更に任意の b について $au=b$ なる u を求めて $eb=eau=au=b$ 即ち $eb=b$，同様にて $be=b$ 即ち単位要素 e が存在する。次に $ax=e$, $xa=e$ を解いて逆要素 a^{-1} が存在する。

第3章 第11節～12節

Sm.9 ◦ 3つの要素からなる体を作る。

[解答] 体は加群であるから零要素0がある。次に体は乗法群を0以外にもつから単位要素eがある。(e≠0 ∵ ea=a より e=0 だとすべての要素が0となる。この体は3つの要素をもつから不合理) eとも0ともちがうこの体の要素を a とする。eとaは乗法群であるから

$ea=ae=a$, $ee=e$, $aa=e$, ($aa=e$ はこの群の位数が2であるから)

なる結合関係を有する。又加法群に対しては位数が3であるから

$0+a=a+0=a$, $e+0=0+e=e$, $0+0=0$,

$a+a+a=0$ は位数3より明らか $a+a\neq a$, $a+a=-a\neq 0$

∴ $a+a=e$, 同様に $e+e=a$

$e+a=e+e+e=0$, $a+e=e+e+e=0$

よって加法群の構造は

$a+0=0+a=a$, $e+0=0+e=0$, $0+0=0$

$a+a=e$, $e+e=a$, $a+e=e+a=0$

となる。次にこれが分配法則を満たすことを証明する。0の積は考える必要がなく。( )内に0がくる時も考える必要はないから。aとeについて証すればよい。eについては e( ) の形は考える必要がないから結局 $a(a+e)$, $a(e+e)$, $a(a+a)$ を調べればよい。(この体は可換であるから) 実際 $a(a+e)=a0=0=aa+ae$,

$a(a+a)=ae=a=aa+aa$, $a(e+e)=e=ae+ae$

が成り立ち明らかに a, e, 0 は体を作る。

Sm.10 ◦ 有限個の要素からなる整域は体である。

[証明] 積 ax に於て a を固定し x を整域Hのすべての要素にわたるようにする。この時 $ax=ay$ なら $x=y$ (→ Sm.2), (但し $a\neq 0$ としておく) だから x と ax は1対1に対応するよって ax は整域Hをつくす。従ってHの任意の要素 y に対して $au=y$ なる u が存在する。xa についても同様にして $ua=y$ なる u の存在がわかる。従ってHは体となる。最初 $a\neq 0$ としたが整域の定義が0以外の零因子をもたないとした時零因子の定義に環には0以外の要素が存在することを仮定しているから当然整域は0以外の要素をもつと仮定している。

§12 準同型, 同型

▷ S, $\bar{S}$ は2つの結合関係をもつ代数系とし, S が $\bar{S}$ の上に写像されるものとする。

準同型 〔$a, b \in S$, $\bar{a}, \bar{b} \in S$ で $a \to \bar{a}$, $b \to \bar{b}$ とする。〕

$$a+b \longrightarrow \bar{a}+\bar{b}$$
$$a \cdot b \longrightarrow \bar{a} \cdot \bar{b}$$

準同型像 $\bar{S}$ … Sの準同型像

▷ 環の準同型像は環である。

[証明] II a) は次から成り立つ。

II $a(bc) = \bar{a} \cdot \bar{b}\bar{c}$ ∴ $\bar{a} \cdot \bar{b}\bar{c} = \bar{a}\bar{b} \cdot \bar{c}$

$(ab)c = \bar{a}\bar{b} \cdot \bar{c}$

I a) $a+(b+c) = \bar{a}+(\bar{b}+\bar{c})$

$(a+b)+c = (\bar{a}+\bar{b})+\bar{c}$

b) $a+b = \bar{a}+\bar{b}$, $b+a = \bar{b}+\bar{a}$ ∴ $\bar{a}+\bar{b} = \bar{b}+\bar{a}$

c) $a+x = b$, $\bar{a}+\bar{x} = \bar{b}$ $\bar{x}$ が存在する。

III a) $a(b+c) = \bar{a}(\bar{b}+\bar{c})$ ∴ $\bar{a}(\bar{b}+\bar{c}) = \bar{a}\bar{b}+\bar{a}\bar{c}$

$ab+ac = \bar{a}\bar{b}+\bar{a}\bar{c}$

b) $(b+c)a = (\bar{b}+\bar{c})\bar{a}$ ∴ $(\bar{b}+\bar{c})\bar{a} = \bar{b}\bar{a}+\bar{c}\bar{a}$

$ba+ca = \bar{b}\bar{a}+\bar{c}\bar{a}$

注) 1. 環が可換ならその準同型像も又可換である。

2. 環が整域であってもその準同型像が整域とは限らない。

3. 環が整域であればその同型像も又整域である。

4. 体の同型な像は体である。

▷ RとS′は、2つの互いに無縁な環とする。さらに、S′はRに同型な部分環R′を含むものとする。するとRを含む環Sで、$S \cong S'$ をみたすものが存在する。

[証明] S′からR′の要素を取り除き、その代りに、同型によってそれと1対1に対応するRの要素を代入する。そして、おきかえられた要素とそうでない要素との和及び積はS′内での和及び積にちょうど対応するようにきめる。こうしてS′から環Sをつくる これは $S \cong S'$ で、実際にRを含んでいる。

商体

§13 商体

▷ 可換環Rがある斜体Ωの中に含まれている時 Rの要素の商をつくることができる。

$$\frac{a}{b} = ab^{-1} = b^{-1}a \qquad (b \neq 0)$$

この時式の演算規則が成り立つ。

$$\begin{cases} \dfrac{a}{b} = \dfrac{c}{d} & \text{は} \quad ad = bc \text{の時} \\ \dfrac{a}{b} + \dfrac{c}{d} = \dfrac{ad+bc}{bd} \\ \dfrac{a}{b} \cdot \dfrac{c}{d} = \dfrac{ac}{bd} \end{cases}$$

これらの証明は両辺に bd を乗じると等しくなることと $bdx = bdy$ から $x=y$ が導けることから明白。
上の規則から 商 $ab^{-1} = b^{-1}a = \frac{a}{b}$ 全体は体（可換体）を作ることがわかる。これを環の商体という。

。 上の演算の定義，や比較は 環Rの中の要素同士の演算によって行なわれるから Rに同型な環の商体はRの商体に同型である。
。特に環Rのつくる2つの商体は同型である。

▷ 可換Rに対して Rが体に埋蔵されるための必要十分条件はRが整域であることである。

[証明]（Rが零環の時を省いて考える。）Rの0以外の要素bで (a, b) のような要素の組全体を考え $ad = bc$ なる時 $(a, b) \sim (c, d)$ と書く。するとこれは反射，対称，推移的である。よって第1章 第5節より 同値な要素 (a, b) を類にまとめれば類別が作られる。(a, b) が属する類を $\frac{b}{a}$ という記号で表わす。この時この演算規則を上の公式にならって定義する。この定義は $b \neq 0, d \neq 0$ ならば $bd \neq 0$ であるから右辺の記号は存在する。又 $\frac{a}{b}, \frac{c}{d}$ は類の代表 $(a, b), (c, d)$ のとり方に関係しないことも証明される（略）
又この類全体が体を作ることも証明される。（略）今Rの要素cに分数 $\frac{c}{1}$ を対応させるとこのような $(b \neq 0)$ 分数は皆等しい。ところが異なった要素 c, c' には異った分数が対応する。よってRとこのような分数は1対1対応をする。又この対応が同型対応であることがわかる。よって前節の定理を使ってRを含むこの分数のつくる体と同型な体ができる。よって環が整域ならばそれを含む体が存在する。
（整域であることは上の証明中 $b \neq 0, c \neq 0$ ならば $bc \neq 0$ に使っている）
又体にRが含まれるためには環が零因子（0以外の）をもってはいけないのは明白

Sm.
商　環

○ 任意の可換環 R（零因子を0以外に含んでもよい）は，bを零因子でないとして，$\frac{a}{b}$ の形のあらゆる商からなる〈商環〉の中に埋蔵される．一般に，Mを零因子を含まない任意の乗法的な集合とする。（$a \in M$ ，$b \in M$ なら $ab \in M$）Mに含まれるbだけをとって $\frac{a}{b}$ を作ると（Mを分母系とする）商環 R_M が得られる。

［証明］　前頁で Rが整域の時 $\frac{b}{a}$ が体をなすことを証明したが，ここでそこでは略したが 体の条件 2）をRを整域として証明する。

$$\frac{b}{a}x = \frac{d}{c} \qquad (c \neq 0,\ a \neq 0,\ b \neq 0)$$

なるxが存在すればよい　xとして $\frac{ad}{bc}$ をとれば

$\frac{b}{a}x = \frac{bad}{abc}$ であるが　$bad \cdot c = abc \cdot d$ であるから

これは $\frac{d}{c}$ に等しい。　$b \neq 0$，$c \neq 0$ であるから　$bc \neq 0$ よって上記方程式の解は存在する。この時 $b \neq 0$，$c \neq 0$ ならば $bc \neq 0$ を使ったがこれは一般に整域に限り成り立つからこれでは整域以外ではつかえない。そこで0以外の零因子を含む環では 上の（除法）xが必ずしも存在しないことを示す。　α を零因子（0以外）とする。するともし分数 $\frac{a}{b}$（bは零因子）で除法が可能なら

$$\frac{\alpha}{b}x = \frac{d}{c}$$

（b，c は 零因子でない。）
（dを零因子以外のある任意の要素とする。）

なるxが存在する。この時 α が零因子であるから $\alpha\beta = \beta\alpha = 0$ なる β が存在する。この β を両辺に乗ずれば（正確には $\frac{\beta r}{r}$ を乗ずる）

$$\frac{\beta\alpha}{b}x = \frac{\beta d}{c}$$

ところが左辺 $\beta\alpha$ は0であるから 左辺は 0となる。（正確には零要素）
依って $\beta d = 0$ となり $\beta \neq 0$ から d は零因子となる。即ち 零因子以外の d について上の方程式は解を分数の環上で有さない。
（環の要素がすべて零因子であればこの証明はなりたたないがそこでは分数が存在しない。）
$\frac{a}{b}$ が環になることは容易に確かめられる。
後者の 証明は略す。

第3章第14節

§14 ベクトル空間と多元環

▷ ベクトル空間

R上のn次元ベクトル空間Gとは

ベクトル空間 ○ 単位要素をもつ環 $R(\alpha, \beta, \cdots)$，アーベル群 $G(u, v, \cdots)$

1. $\alpha \in R$ と $u \in G$ に対して $\alpha u \in G$
2. $\alpha(u+v) = \alpha u + \alpha v$
3. $(\alpha+\beta)u = \alpha u + \beta u$
4. $(\alpha\beta)u = \alpha(\beta u)$
5. Gのすべての要素は，n個の〈基底〉$u_1, u_2, \cdots, u_n$ により，1次形式 $\alpha_1 u_1 + \cdots + u_n u_n$ の形に，1通りに表わせる。

基底

注） Gを R に関するn項線型加群ともいう。

線型加群

○ 上記法則より

(1) $\beta(\alpha_1 u_1 + \cdots + \alpha_n u_n) = (\beta\alpha_1)u_1 + \cdots + (\beta\alpha_n)u_n$

(1)′ $1 \in R$ に対し $1 \cdot u = u$

(2) $(\alpha_1 u_1 + \cdots + \alpha_n u_n) + (\beta_1 u_1 + \cdots + \beta_n u_n)$
$= (\alpha_1+\beta_1)u_1 + (\alpha_2+\beta_2)u_2 + \cdots + (\alpha_n+\beta_n)u_n$

○ $u_1, \cdots, u_n$ をGの基底とする時n個の要素の列 $(\alpha_1, \alpha_2, \cdots, \alpha_n)$ と $u = \alpha_1 u_1 + \cdots + \alpha_n u_n$ は1対1に対応するがこの α_i を u の基底 $u_1, \cdots, u_n$ に対する成分という。

成分

▷ ベクトル空間は，環Rと次元nを指定すれば，同型を除いてただ1通りにきまる。

注） Rのn個の要素の順序のつにた列 $(\alpha_1, \cdots, \alpha_n)$ をベクトルと考えるとそれらは R上のn次元ベクトルのすべてと同型でであるから1つのモデルとなる。

▷ 多元環

多元環 Gの要素間に乗法が定義されている。Gが環となり更に

(3) $\alpha \in R$ に対して $(\alpha u)v = u(\alpha v) = \alpha(uv)$

なるGを多元環（環R上の階数nの）という。

これから $\left(\sum_j \alpha_j u_j\right)\left(\sum_k \beta_k u_k\right) = \sum_j \sum_k \alpha_j \beta_k (u_j u_k)$

$$u_j u_k = \sum_l \gamma_{jk}^l u_l$$

構造定数　の定数 γ_{kj}^l を 群元環 G の構造定数とよぶ

注）γ_{kj}^l を任意にとっても 分配法則を満たす，R が可換なら (3) も満たす。

よって

$$u_j(u_k u_l) = (u_j u_k) u_l$$

が満たされるように γ_{jk}^l がきまれば G は 群元環となる。

- R が可換で u_j のかけ算も可換なら G も可換となる。

G が単位要素 e を含んでいるとその倍要素 αe は G の中で R に同型な環をなすのでそれを R の要素 α と同一視してもさしつかえない。

群元体　G が斜体になる時 群元体ともいう。

複素数体
- 複素数体　R… 実数体R，Gの基底 e，i

$$e\cdot e = e,\quad e\cdot i = i,\quad i\cdot e = i,\quad i\cdot i = -e$$　C

ガウスの数体
- ガウスの数体　R… 有理数体P．G 基底は上に同じ　P(i)

ガウスの整数環
- ガウスの整数環　R… 有理整数環 Z　基底は上に同じ　Z(i)

四元数体
- 四元数体　R… 実数体R又は有理数体P，基底 e, j, k, l,　Q

$ee=e$，$jj=kk=ll=-e$，$ej=je=j$，$ek=ke=k$，$el=le=l$

$jk=l$，$kj=-l$，$kl=j$，$lk=-j$，$lj=k$，$jl=-k$

注）a,b,c,d を実数 ae を a と同一視できる要素 $a+bj+ck+dl$ を四元数という。

群環
- 群環 ベクトル空間 R_G の基底に，有限群 G の要素をとると 群元環 R_G ができる これを，G の R 上での群環という。

▷ 無限階の群元環

無限個の基底 $u_1, u_2, \cdots, \cdots$ に対して そのうち有限個の基底をとり出した $\sum \alpha_j u_j$ を考える。このような環に対しても前に述べたことはすべて成り立つ。

Sm1
- 環 R の n^2 個の要素 α_{jk} ($j=1,\cdots,n$; $k=1,\cdots,n$,) の組を，n 次の行列と定義し 2つの行列 (α_{jk})，(β_{jk}) の和 (σ_{jk}) と積 (τ_{jk}) を次のように決める。

第3章 第14節

$$\sigma_{jk} = \alpha_{jk} + \beta_{jk}, \quad \alpha(\alpha_{jk}) = (\alpha\alpha_{jk})$$

$$\pi_{jl} = \sum_{k=1}^{n} \alpha_{jk}\beta_{kl},$$

すると n 次の行列全体は，R 上の階数 n^2 の多元環［n 次の完全行列環］を作る。

完全行列環

［証明］ $\alpha(\alpha_{jk}) \in G$ より 1 は成立，2 は．

$$\alpha(\alpha_{jk}+\beta_{jk}) = \alpha(\gamma_{jk}) = (\alpha\gamma_{jk})$$

$\gamma_{jk} = \alpha_{jk}+\beta_{jk}$ より 2 も成立

$$(\alpha+\beta)(\alpha_{jk}) = \{(\alpha+\beta)\alpha_{jk}\} = \{\alpha\alpha_{jk}+\beta\alpha_{jk}\}$$
$$= \alpha(\alpha_{jk}) + \beta(\alpha_{jk}) \quad \text{より 3 も成立},$$

$(\alpha\beta)(\alpha_{jk}) = (\alpha\beta\alpha_{jk}) = \alpha(\beta\alpha_{jk})$ より 4 も成立

$\alpha_{jk}=1$，それ以外は皆 0 として u_{jk} を作ると。

$(\alpha_{jk}) = \sum \alpha_{jk}u_{jk}$ とする。 より 5 も成立

$(\alpha_{jk})(\beta_{jk}) = (\pi_{jk})$，$(\beta_{jk})(\gamma_{jk}) = (\delta_{jk})$ とする

$(\pi_{jk})(\gamma_{jk}) = (\rho_{jk})$，$(\alpha_{jk})(\delta_{jk}) = (\lambda_{jk})$ とする。

$$\rho_{jl} = \sum_{k=1}^{n} \pi_{jk}\gamma_{kl} = \sum_{k=1}^{n}\left\{\sum_{s=1}^{n}\alpha_{js}\beta_{sk}\right\}\gamma_{kl}$$
$$= \sum_{k=1}^{n}\sum_{s=1}^{n}(\alpha_{js}\beta_{sk}\gamma_{kl})$$

同様に

$$\lambda_{jl} = \sum_{k=1}^{n}\sum_{s=1}^{n}(\alpha_{js}\beta_{sk}\gamma_{kl}) \quad \therefore (\rho_{jl}) = (\lambda_{jl}) \text{ 結合法則成立。}$$

$(\alpha_{jk})\{(\beta_{jk})+(\gamma_{jk})\} = (\rho_{jk})$ とおく

$$\rho_{jl} = \sum_{k=1}^{n}\alpha_{jk}(\beta_{kl}+\gamma_{kl}) = \sum_{k=1}^{n}\alpha_{jk}\beta_{kl} + \sum_{k=1}^{n}\alpha_{jk}\beta_{kl}$$

$\therefore (\rho_{jk}) = (\alpha_{jk})(\beta_{jk}) + (\alpha_{jk})(\gamma_{jk})$ 分配法則成立

もう一方も同様にして成立。

$$\{\alpha(\alpha_{jk})\}(\beta_{jk}) = \left(\alpha\sum_{s=1}^{n}\alpha_{js}\beta_{sk}\right)$$
$$= (\alpha_{jk})\{\alpha(\beta_{jk})\}$$
$$= \alpha\{(\alpha_{jk})(\beta_{jk})\}$$

よって (3) も成立 故に多元環とする。

Sm. 2

- 2 次の複素行列

$$\begin{pmatrix} a+ib & c+id \\ -c+id & a-ib \end{pmatrix}$$

は四元数体に同型な多元環を作る。

［証明］ この形の和はこの形 積は

$$\begin{pmatrix} a+ib & c+id \\ -c+id & a-ib \end{pmatrix}\begin{pmatrix} a'+ib' & c'+id' \\ -c'+id' & a'-ib' \end{pmatrix}=\begin{pmatrix} A+Bi & C+iD \\ -C+iD & A-iB \end{pmatrix}$$

$A = aa'-bb'-cc'-dd'$, $B = ab'+a'b+cd'+c'd$

$C = ac'-bd'+ca'+db'$, $D = ad'+bc'+a'c-b'c$

となりこの形である。先の証明で行列の和，積がもとの行列になること及び行列の和，積の定義を使ったのだから先の証明は有効である。従ってこの形は環である。但し5だけは別に証明する必要がある。

それには

$$u_1=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\quad u_2=\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix},\quad u_3=\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},\quad u_4=\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

をとれば十分である。更に

$u_1u_2 = u_2u_1 = u_2$, $u_1u_3 = u_3u_1 = u_3$, $u_1u_4 = u_4u_1 = u_4$

$u_1^2 = u_1$, $u_2^2 = u_3^2 = u_4^2 = -1$, $u_2u_3 = u_4$, $u_3u_2 = -u_4$

$u_3u_4 = u_2$, $u_4u_3 = -u_2$, $u_4u_2 = u_3$, $u_2u_4 = -u_3$

が成り立つ。Rは実数体である。

今 $u_1 \to e$, $u_2 \to j$, $u_3 \to k$, $u_4 \to l$ の対応を考えると四元数体と2次の複素行列に1対1の対応がつく更に基底の構造が同じだから四元数体と複素行列は同型となる。

注）このことから四元数の乗法の結合法則が簡単に証明された。

§15 多項式環

多項式環

- Rを単位要素をもつ環で，Gは1つの要素 x の累乗からなる無限巡回群であるとする。Gの要素 x^μ を多元環の基底に用いる。

その一つの要素

$$\sum a_\nu x^\nu$$

多項式 を，R上の多項式という。

不定元 x …… 不定元

係数 a_ν …… 多項式の係数

(1)
$$\begin{cases} \sum a_\nu x^\nu + \sum b_\nu x^\nu = \sum (a_\nu+b_\nu)x^\nu \\ (\sum a_\lambda x^\lambda)(\sum b_\lambda x^\lambda) = \sum c_\nu x^\nu \end{cases}$$

但し $c_\nu = \sum_{\lambda+\mu=\nu} a_\lambda b_\mu$

第3章 第15節

▷ 不定元 x を付加する …… 環 R から 多項式環 $R[x]$ を作る。

多項式環 $R[x_1, \cdots, x_m]$ …… $\sum a_{\alpha_1 \cdots \alpha_m} x_1^{\alpha_1} \cdots x_m^{\alpha_m}$ 全体
整係数多項式 … R が有理整数環 $\mathbb{Z}$

▷ 不定元に環の要素を代入する。

α が R のすべての要素と可換な（R あるいは R の拡大環）の要素である時 多項式 $f(x)$ の式の中の x を皆 α におきかえることができ 値 $f(\alpha) = \sum a_\nu \alpha^\nu$ が得られる。

$f(x) + g(x) = s(x)$ ならば $f(\alpha) + g(\alpha) = s(\alpha)$ は明白

$f(x)\,g(x) = p(x)$ ならば $p(\alpha) = \sum c_\nu \alpha^\nu = \sum_\nu \sum_{\lambda+\mu=\nu} a_\lambda b_\mu \alpha^\nu$

$= \sum_\lambda \sum_\mu a_\lambda b_\mu \alpha^{\lambda+\mu} = (\sum a_\lambda \alpha^\lambda)(\sum b_\mu \alpha^\mu) = f(\alpha)\, g(\alpha)$

$\therefore \quad f(\alpha)\, g(\alpha) = p(\alpha)$

- 多項式 $f(x)$, $g(x)$, … の間に成り立つ，加法と乗法についてのすべての関係は，x に 環 R のすべての要素と可換な要素 を代入しても変わらない。これは 2つ以上の不定元の多項式にも成り立つ。
  特に R が可換なら R のかってな要素を代入することができる。

有理整函数
- 多項式 …… 変数 $x_1, \cdots, x_n$ の有理整函数ともいう。

注） $a \in R$ に対し ax^0 は a と同一視できるよって $R \in R[x]$

- 定数項のない整係数多項式には x にどんな環の要素を代入してもよい。

▷
- R が整域なら $R[x]$ も整域である。
- R が整域なら 積 $f(x)\,g(x)$ の次数は，$f(x)$ の次数と $g(x)$ の次数との和に等しい。
- R が整域なら $R[x_1, \cdots, x_n]$ も整域である。
- 同次多項式 項 $a_{\alpha_1 \cdots \alpha_r} x_1^{\alpha_1} \cdots x_r^{\alpha_r}$ の次数 $\sum \alpha_i$ が皆等しい多項式（形式ともいう）

▷ 割り算 R を単位要素 1 をもつ環とする。

割り算 $g(x) = \sum c_\nu x^\nu$ $(c_m = 1)$ $\deg g(x) = n$, $\deg$ は次数を示す
$\deg f(x) = m \geqq n$ とする。f から g の倍元 $a_m x^{m-n} g$ をひいて f の最高次の係数を0にすることができる。（$f(x) = \sum a_\mu x^\mu$）
これを続けると $f - gq = r$, $0 \leqq \deg r < \deg g$
にるこの演算を割り算と定義する。

Rが斜体の時は $g \neq 0$ の時 $C_m = 1$ なる仮定は いらない。

Sm ○ $x, y, \cdots$ を無限個の記号とすると，これらを不定元とする R の多項式全体を考えることができる。但し各多項式はこれらの不定元を有限個しか含まないものとする。こうして定義された領域は，R が環なら環になるし R が整域ならやはり整域になる。（但し R は単位要素 1 をもっているとする）

［証明］ 基底の積が結合法則と前節 (3) を満たすことを R が環であることから導けばよい。基底 $x_{p_1}^{\alpha_1} \cdots x_{p_m}^{\alpha_m}$ と $x_{q_1}^{\beta_1} \cdots x_{q_m}^{\beta_m}$ の積に於て両方にでてくる不定元を $x_{r_1}, \cdots, x_{r_s}$ とかく。

$x_{p_1}^{\alpha_1} \cdots x_{p_m}^{\alpha_m}$ を $x_{r_1}, \cdots, x_{r_s}$ の積と考え x_{r_k} が含まれない時は $r_k = 0$ として形式的に積にそえれば $x_{p_1}^{\alpha_1} \cdots x_{p_m}^{\alpha_m} = x_{r_1}^{\delta_1} \cdots x_{r_s}^{\delta_s}$，$x_{q_1}^{\beta_1} \cdots x_{q_m}^{\beta_m} = x_{r_1}^{\varepsilon_1} \cdots x_{r_s}^{\varepsilon_s}$ とおり積は $x_{r_1}^{\delta_1+\varepsilon_1} \cdots x_{r_s}^{\delta_s+\varepsilon_s}$ となる更にこの積を3つにして同様にすれば $x_{r_1}^{\alpha_1+\beta_1+\gamma_1} \cdots x_{r_s}^{\alpha_1+\beta_1+\gamma_1}$ ここで α_i は最初の基底の指数 β_i は2番目の基底の指数 γ_i は3番目の基底の指数となり $(\alpha_i+\beta_i)+\gamma_i = \alpha_i+(\beta_i+\gamma_i)$ から基底の積が結合法則を満たすことがわかる。

$(\alpha u)v = u(\alpha v) = \alpha(uv)$ を証明する。これは基底にのみ証明されれば十分である。因数の含む不定元を $x_{p_1}, x_{p_2} \cdots, x_{p_m}$ とする

$$(\alpha\, \alpha_{p_1\alpha_1} \cdots {}_{p_m\alpha_m}\, x_{p_1}^{\alpha_1} \cdots x_{p_m}^{\alpha_m})(\alpha_{p_1\beta_1} \cdots {}_{p_m\beta_m}\, x_{p_1}^{\beta_1} \cdots x_{p_m}^{\beta_m})$$

$$= \alpha\, \alpha_{p_1\alpha_1} \cdots {}_{p_m\alpha_m}\, \alpha_{p_1\beta_1} \cdots {}_{p_m\beta_m}\, x_{p_1}^{\alpha_1+\beta_1} \cdots x_{p_m}^{\alpha_m+\beta_m}$$

$u(\alpha v)$ も $\alpha(uv)$ もこれになるから (3) は証明された。

よって $R[x, y, \cdots]$ は多元環となる。

R が整域なら $f(x_1, \cdots, x_m)$，$g(x_1, \cdots, x_m)$（但し $x_1, \cdots, x_m$ は f, g にある不定元を列挙したもので f の中には $x_1, \cdots, x_m$ が全部ある必要はない g についても同様）

f の次数最高の項 $\alpha x_1^{p_1} \cdots x_m^{p_m}$ のうち p_1 が一番大きなものをとる。これが1個でなければ順次 p_1, p_2, p_3 と下っていきそれぞれの1番大きい項をとる。このようにして上の意味で最高の項 $\alpha x_1^{p_1} \cdots x_m^{p_m}$ が f にも，g にも右確定する。（但し $f \neq 0$，$g \neq 0$ の仮定のもとで）

この時 f の最高の項を $\alpha x_1^{p_1} \cdots x_m^{p_m}$，$g$ の最高の項を $\beta x_1^{q_1} \cdots x_m^{q_m}$ とすれば fg の最高の項は $\alpha\beta x_1^{p_1+q_1} \cdots x_m^{p_m+q_m}$ である。（証明略）

よって $\alpha \neq 0$，$\beta \neq 0$ であるから $\alpha\beta \neq 0$ 即ち $f \neq 0$，$g \neq 0$ なら $fg = 0$

第3章 第16節

§16 イデアル，剰余環

▷ 環Rの部分環S

部分環

1. Rの加法群の部分群である。（$a \in S, b \in S$ ならば $a-b \in S$）
2. $a \in S, b \in S$ ならば $ab \in S$ （乗法集合）

▷ 環Rのイデアル $\mathfrak{m}$ （右イデアル）

イデアル
右イデアル
左イデアル
両側イデアル

1. $a \in \mathfrak{m}$, $b \in \mathfrak{m}$ ならば $a-b \in \mathfrak{m}$ （部分加群）
2. $a \in \mathfrak{m}$, $r \in R$ ならば $ar \in \mathfrak{m}$ <右倍元を含む>

（2が $ra \in \mathfrak{m}$ となる時は左イデアル，両方成り立てば両側イデアルという）

注） Rが可換の時上述3種のイデアルは一致し単にイデアルという
この節では特に断わらない限りRは可換であるとする。

0イデアル
単位イデアル
単項イデアル

- 0イデアル … 零要素だけから成るイデアル
- 単位イデアルR … 環Rのすべての要素からなる。
- 1つの要素aから生成されるイデアル（a），これは （単項イデアルという）

$$ra + na \quad (r \in R, n \text{は有理整数})$$

の形の要素全体から成る。環Rが単位要素eを含めばこの式は単に ra （$r \in R$）となる。（$\because na = ne \cdot a$ となる）

- 多くの要素 $a_1, a_2, \cdots, a_m$ から生成されるイデアル

$$\sum r_i a_i + \sum n_\lambda a_\lambda \quad (r_i \in R, n_\lambda \text{は有理整数})$$

イデアル基底

このイデアルを $(a_1, \cdots, a_m)$ と書き $a_1, \cdots, a_m$ はイデアル基底をなすという。

- 無限個の要素から成る集合Mから生成されるイデアル（M）は

$$\sum r_i a_i + \sum n_\lambda a_\lambda \quad (a_i \in M, r_i \in R, n_\lambda \text{は整数})$$

の形の有限和全体となる。

注） 0イデアルは（0）とかける。又Rが単位要素eをもてば単位イデアルは（e）とかける。

▷ 剰余類 Rをそのイデアル（部分加群）$\mathfrak{m}$ によって剰余類に分ける。

2つの要素の差 $a-b$ が $\mathfrak{m}$ に属す時 a, b は $\mathfrak{m}$ に関して合同であるといい $a \equiv b \pmod{\mathfrak{m}}$ 又は $(\mathfrak{m})$ と書く

注） $\mathfrak{m} = (m)$ の時は $a \equiv b \pmod{m}$ と書くことが多い。

合同式 ▷ 合同式の計算 （法はすべて イデアル $\mathfrak{m}$ とし 簡単のため記さない）

○ $a \equiv a'$, $b \equiv b'$ ならば

1. $a+b \equiv a+b' \equiv a'+b'$ （又は $a-b \equiv a'-b'$）

2. $ab \equiv ab' \equiv a'b'$

注） 和，積については 上から普通の計算と同じであるが 簡約は一般にできない。（Rが整域であっても）

Sm 1. ○ 有理整数環 $\mathbb{Z}$ では，イデアル (m) $(m>0)$ を法とする剰余類は，数 $0, 1, \cdots, m-1$ によって代表できそれらを $C_0, C_1, \cdots, C_{m-1}$ で表わすことができる。

［証明］ 任意の整数 a を $mp+r$ $(0 \leqq r < m)$ の形に書くと

$a \in mp+r+(m) = r+(m)$ 即ち $0 \leqq r < m$ によって代表される。

又 $0 \leqq r_1, r_2 < m$ とし $r_1 \neq r_2$ とする時

$r_1+(m) = r_2+(m)$

となることはない。（∵ $r_1+(m) = r_2+(m)$ だと $r_1-r_2 \in (m)$ となる）

よって剰余類の代表として $0, 1, \cdots, m-1$ をとれる。

それぞれの代表する剰余類を $C_0, C_1, \cdots, C_{m-1}$ とし

$C_u + C_v = C_{u+v} = C_w$

を $u+v \equiv w \ (m)$ $(0 \leqq w < m)$ で定義する。

積についても

$C_u \cdot C_v = C_{uv} = C_w$

$uv = w \ (m)$ $(0 \leqq w < m)$ で定義する。

Sm. 2 ○ 有理整数環 $\mathbb{Z}$ で 2つの数 10と13とは，どんなイデアルを生成するか。

［解答］ そのイデアル $(10, 13)$ は $10a+13b$ の形の整数全体である。$10a+13b$ は 1を含むから $(10 \cdot 4 + 13 \cdot (-3))$ そのイデアルは単位イデアルとなる。即ち有理整数環 $\mathbb{Z}$ 自身となる。

Sm 3 ○ $a \equiv b \ (0)$ は，どういうことを表わすか。

［解答］ (0) は零要素しか含まれないからこれは $a-b=0$（零要素）即ち $a=b$ であることを示している。

Sm 4 ○ 要素 a のすべての倍元 ra $(r \in R)$ はイデアル Ra を作るこのイデアルは必ずしも単項イデアル (a) とは一致しない。

［証明］ Rとして 偶数の作る環をとる。この時 単項イデアルは $ra+ma$ (m は整数)の形となる従って (a) は pa $(p \in \mathbb{Z})$ の全体と一致する。

ところが Ra は ra $(r \in R)$ となり $R \subset \mathbb{Z}$ であるから両方は一致しない。

第8章第16節

Sn. 5 ○ 可換でない環に，任意の集合から生成される右イデアル（左イデアル），両側イデアルを定義する。

［解答］ まず任意の集合 G を有限集合と仮定し G の要素を $a_1, a_2, \cdots, a_m$ とする。右イデアルを作る。

和 $\sum a_i r_i + \sum n_\alpha a_\alpha$ を作る。するとこれが加群をつくることが容易にわかる。又 $s \in R$（Rとにる環）をこの両辺に乗じると

$$\sum a_i r_i s + \sum n_\alpha a_\alpha s = \sum a_i (r_i s + n_i s) + \sum 0\, a_\alpha$$

となりこれは明らかにイデアルとなる又 G を含むイデアルは $a_i r_i$ と $n_\alpha a_\alpha$ を含まなくてはならないからこれは G から生成される右イデアルである。

（同様にて左イデアルは $\sum r_i a_i + \sum n_\alpha a_\alpha$ の形全体となる。）

両側イデアルは左右のイデアルが一致する場合である。

Sn 6 G が無限集合の時はそれぞれの有限和として上の式を用いればよい。

Sn 6 ○ 可換でない環に於て合同式にどのような計算が許されるか。

［解答］ $\mathfrak{m}$ を R（非可換の環）の右イデアルとする

R は非可換でも和については可換であるから。和については可換の R と同じことが成り立つ。積については $a \equiv a' \ (\mathfrak{m})$ $b \equiv b' \ (\mathfrak{m})$ とする時

$$ab \equiv a'b \ (\mathfrak{m})$$
$$ba \equiv b'a \ (\mathfrak{m})$$

は成り立つが一般に $ab \equiv a'b' \ (\mathfrak{m})$ は成り立たない。

従って 一般に $a \equiv a' \ (\mathfrak{m})$ が与えられた時 任意の要素 C について

$$ac \equiv a'c \ (\mathfrak{m}) \qquad (c \in R)$$

が許されるだけである。左イデアルに対しては $a \equiv a' \ (\mathfrak{m})$ に対して

$$ca \equiv ca' \ (\mathfrak{m}) \qquad (c \in R)$$

が成り立つ。又両側イデアルに対しては記号は先と同じにして

$$ab \equiv a'b \equiv a'b' \ (\mathfrak{m})$$

よって両側イデアルに対して可換な環 R の時と同じ計算が許される。

▷ 環の準同型

2つの環の準同型 $R \sim \overline{R}$ によって環 R に1つの類別が定義される即ち．同じ像をもつすべての要素 a を1つの類 C(a) にまとめる。

○ 準同型 $R \sim \overline{R}$ によって，$\overline{R}$ の零要素が対応する R の類 $\mathfrak{n}$ は，R のイデアルで他はこの剰余類である。（証明は P26 の群の時と同様にてなされるので省略） （なお次々頁 Sn 10 の証明を参照）

○ 群の時と同様にて R のイデアル $\mathfrak{m}$ の剰余類は環をつくる。その際2つの剰余類の積，和はその中に含まれる任意の2要素をとって計算を行ないその属する剰余類をその剰余類の和，積と定義する。
（もちろん群の時と同様に $\mathfrak{m}$ の剰余類の和，積はそのとる2つの要素によらないことが証明される）これを R の $\mathfrak{m}$ に関する剰余環 あるいは $\mathfrak{m}$ を法とする R の剰余環という。 記号 $R/\mathfrak{m}$ で表わす。 R と $R/\mathfrak{m}$ は準同型対応をする。特に $R/\mathfrak{m}$ の零要素に対応する R の要素 全体は $\mathfrak{m}$ となる。

剰余環

▷ 環の準同型定理

これから準同型 $R \sim \bar{R}$ に対してその零要素に対応するイデアル $\mathfrak{n}$ の剰余類と $\bar{R}$ の要素が1対1に対応し $\mathfrak{n}$ の剰余類全体が環になることがわかった。この $\bar{R}$ と $R/\mathfrak{n}$ の1対1の対応は実は同型である。
即ち剰余類 $C(a)$，$C(b)$ の和，積は $C(a+b)$，$C(ab)$ で R の要素 $\bar{a}$，$\bar{b}$ の和，積は $\overline{a+b}$，$\overline{ab}$ だからである。
よって次の（環の第1準同型）定理が成り立つ

▷ R に準同型な環 $\bar{R}$ は，1つの剰余環 $R/\mathfrak{n}$ に同型である。ここで $\mathfrak{n}$ は $\bar{R}$ における像が0であるような要素の作るイデアルである。逆にすべての剰余環 $R/\mathfrak{n}$ は R に準同型である。

Sm.7 ○ 環 R が零因子をもたなくても，その剰余環 $R/\mathfrak{m}$ が零因子をもつことがありうる。
［証明］ いい方をかえれば環 R に零因子がなくても イデアル $\mathfrak{m}$ に属さない2つの要素の積がイデアル $\mathfrak{m}$ に属すことがある。という定理（ここで零因子は0以外の零因子をさしている）である。このような例は R を整数環 $\mathbb{Z}$ とし例えば $2\times3=6$ の (6) を考えれば 2 ∉ (6)，3 ∉ (6) であるのに $2\cdot3 \in (6)$ である 従って剰余環では $C_2 \cdot C_3 = 0$，$C_2 \neq 0$，$C_3 \neq 0$

Sm.8 ○ 準同型 $R \sim \bar{R}$ が同型であるためには $\mathfrak{n}=(0)$ であることが必要十分である。
［証明］ $R \sim \bar{R}$ が同型であることと $R \sim R/\mathfrak{n}$ が同型になることは同じことであるから $\mathfrak{n}=(0)$ が $R \sim R/\mathfrak{m}$ が同型になることの必要十分条件であることがいえればよい。もし $R \sim R/\mathfrak{n}$ が同型でなければ

$$a \equiv b \ (\mathfrak{n}) \qquad (a \neq b)$$

である a，b が存在する。ところが $\mathfrak{n}=(0)$ だから Sm.3 より $a=b$ となって仮定に反す 従って $\mathfrak{n}=(0)$ は十分条件である。
これが必要条件であるのは $\bar{R}$ の零要素に対応する R の要素が0だけでなくてはならないから明らかである。

第3章 第16節

Sn.9 ○ 体には0イデアルと単位イデアルの他にイデアルは存在しない。又体の準同型はこれからどういうことがわかるか。（体は斜体のことである）

[証明] 斜体の1つのイデアルに零以外の要素 a が存在したとする。この時体の要素 a^{-1} と a との積 e はイデアルに属するからこのイデアルは単位イデアルとなる。0要素だけはもちろんこれだけでイデアルを作る。この結果から体Rの準同型像 $\overline{R}$ が存在したとすればそれは，体Rに同型である（$m=(0)$）か零環であるかである。

Sn.10 ○ 可換でない環に於ては，準同型な像はかならず両側イデアルによって作られる。逆に，すべての両側イデアルは実際剰余環をもつ。

[証明] 非可換な環Rの準同型 $R\sim\overline{R}$ があったとする。この $\overline{R}$ の零要素に写像されるRの要素は両側イデアルをつくる。

$\because$ $a\to\overline{0}$，$b\to\overline{0}$ ならば $-b\to\overline{0}$ で $a-b\to\overline{0}$ であるからこれらは加群である。 $a\to\overline{0}$ ならば $\forall\gamma\in R$ に対して $\gamma\cdot a\to\overline{\gamma}\cdot\overline{0}=\overline{0}$，$a\cdot\gamma\to\overline{a}\overline{\gamma}=\overline{0}$ となりこれらは両側イデアルとなる。これを m と書く 剰余類 $c+m$ はすべて同じ要素 $\overline{c}$ に写像される。又 $b\to\overline{c}$ ならば $b-c\to\overline{0}$ よって $b\equiv c\ (m)$ 即ち 剰余類 $c+m$ と $\overline{R}$ の要素 $\overline{c}$ とは1対1に対応する。次に剰余類 $a+m$ を $\overline{a}$ で表わす。剰余類の積 $\overline{a}\overline{b}$ をその両方に属する2つの要素の積の属する剰余類と定義する。するとこの時その2つの要素のとり方に，剰余類の積は影響されない。（$\because$ $a\equiv a'\ (m)$ $b\equiv b'\ (m)$ ならば $ab\equiv a'b'\ (m)$）和についても同様に定義する。（$a\equiv a'\ (m)$ $b\equiv b'\ (m)$ ならば $a+b\equiv a'+b'\ (m)$ であるから上と同じ）このようにすると Rの要素 a に対して $\overline{a}$ が対応し Rの要素の和 $a+b$，積 ab に対して剰余類の和 $\overline{a+b}$ 積 $\overline{ab}$ が対応するからこの対応は準同型で 剰余類 $c+m$ は剰余環 R/m となる。又前と同じ（前頁）ようにしてすべての準同型像 $\overline{R}$ は剰余環 R/m と同型になる。よって定理は成り立つ。

Sn.11 ○ ガウスの整数 $a+bi$ の環 $Z[i]$ は不定元 x の有理整係数多項式環 $Z[x]$ の，イデアル (x^2+1) を法とする剰余環に同型である。

[証明] $Z[x]$ の要素 $f(x)$ は“割り算”によって必ず $f(x)=p(x)(x^2+1)+bx+a$ の形となる。よって $Z[x]/(x^2+1)$ のそれぞれの代表は $bx+a$ の形で表わせるがこのうち $a\equiv a'$，$b\equiv b'$ ならばどの2つも同じ剰余類に属さないから $bx+a$ はそのままそれが $Z[x]/(x^2+1)$ の要素を代表する。$bx+a$ の属する剰余類 $C(a\,b)$ に対して $a+bi$ なるガウスの整数を対応さすとこの対応は1対1である。剰余類 $C(a\,b)$ と $C(a'\,b')$ との和は $C(a+a',\ b+b')$ であり

積については　$bx+a$ と $b'x+a'$ を代表にとってかけ合わせてみると

$$bb'x^2+(ab'+a'b)x+aa' \equiv (ab'+a'b)x+aa'-bb' \quad (x^2+1)$$

であるから

$$c(a,b)\,c(a'b') = c(aa'-bb', ab'+a'b)$$

となる。これは　ガウスの整数の積

$$(a+bi)(a'+b'i) = (aa'-bb')+(ab'+a'b)i$$

に対応するよってこの対応は同型である。

整除

§17　整除と素イデアル

▷ ○ a はイデアル b で割りきれる …… $a \equiv 0\ (b)$

割りきれる ○ イデアル a はイデアル b で割りきれる …… $a \in a$ に対して　$a \equiv 0\ (b)$ で　$a \equiv 0\ (b)$ と書く

約イデアル ○ 約イデアル　上述の b を a に対していう。即ち　$b \geq a$

倍イデアル ○ 倍イデアル　上述の a を b に対していう。即ち　$a \leq b$

真の約イデアル ○ 真の約イデアル　上述 b が　$b \supset a$ 即ち　$b \neq a$ の時

真の倍イデアル ○ 真の倍イデアル　上述 a が　$a \subset b$ 即ち　$a \neq b$ の時

素イデアル ○ R の素イデアル p …… 剰余環 R/p が整域となるイデアル

単位イデアルは素イデアルとみる。

0イデアルは環 R そのものの整域であるか否かに一致する。

極大イデアル ○ R の極大イデアル p …… 単位イデアル以外の真の約イデアルがないイデアル

注）上述イデアルを作る R は常に環としている。（素イデアル以下考える環は皆可換とする。）

▷ 単位要素 e をもつ環 R においては，R と異なる極大イデアル p は素イデアル p であり，しかもその剰余環 R/p は体である。逆に R/p が体ならば p は極大である。

［証明］　剰余環 R/p の中で方程式 $x\bar{a}=\bar{b}$ を解く。但し $a \not\equiv 0\ (p)$ で b は任意であるとする。p と a はひとつのイデアルを生成するがそれは p の真の約イデアルであるから単位イデアルに等しい。よって R の要素 b は $b=p+\gamma a$ （$p \in p$，$\gamma \in R$）と表わせる。（R が単位要素を含むからこう表わせる）この両辺を準同型対応によって剰余環 R/p に写すと。

$\bar{b}=\bar{\gamma}\bar{a}$　即ち方程式 $x\bar{a}=\bar{b}$ がとけた。よって R/p は体である。

第3章 第17節

体は0以外の零因子を含まないから $R/\mathfrak{p}$ は当然素イデアルである。
逆に $R/\mathfrak{p}$ が体であれば $\mathfrak{a}$ は $\mathfrak{p}$ の真の約イデアルとし a は $\mathfrak{p}$ に含まれない $\mathfrak{a}$ の要素とすると 合同式

$$ax \equiv b \quad (\mathfrak{p})$$

は R のすべての b について解をもつ. これから

$$ax \equiv b \quad (\mathfrak{a})$$
$$0 \equiv b \quad (\mathfrak{a})$$

となるが b は R のかってな要素だから $\mathfrak{a} = R$ である。

Sm. 1. ○ 整係数多項式環 $\mathbb{Z}[x]$ のイデアル (x) は イデアル $(2, x)$ をその真の約イデアルにもっている。イデアル (x) も $(2, x)$ も素イデアルである。

[証明] イデアル (x) は 多項式 $f(x)x$ の全体を指す。イデアル $(2, x)$ は 多項式 $2g(x) + xf(x)$ の全体を指す。よって $(2, x)$ は (x) の真の約イデアルデアルである。

剰余環 $\mathbb{Z}[x]/(x)$ を考える。それらは代表に整数 a をつけることができる。$\because f(x) = xp(x) + a$ よって剰余類の演算は整数の演算に一致し従って零因子を有しないから (x) は素イデアルである。

一方 $f(x) = xp(x) + 2m + c$ $(c = 0, 1)$ とかけるから $\mathbb{Z}[x]/(2, x)$ の剰余類の演算は $0+1=1$, $0+0=0$, $1+1=0$, $0\cdot1=1$, $1\cdot1=1$, $0\cdot0=0$ で行なわれるが明らかにこれは0以外の零因子をもたないから素イデアルである。

Sm 2 ○ 有理整数環 $\mathbb{Z}$ に於て (2) と (3) は素イデアルである。

[証明] イデアル (2) は 2η $(\eta \in \mathbb{Z})$ 全体を指すから すべての整数が $a = 2m + c$ $(c = 0, 1)$ と表わせることから $\mathbb{Z}/(2)$ の代表は 0と1で表わせる。 $a \equiv 1$ (2) $b \equiv 0$ (2) なら $ab \equiv 0$ (2)
$a \equiv 1$ (2), $b \equiv 1$ (2) ならば $ab \equiv 1$ (2), $a \equiv 0$ (2), $b \equiv 0$ (2) ならば $ab \equiv 0$ (2), よって剰余類 (2) 以外零因子は存在しない。
よって (2) は素イデアル。 (3) は代表に $0, 1, 2$ をとり演算はすべてこれらの積で行なわれるから, この演算に於て $a \not\equiv 0$ $b \not\equiv 0$ に対し $ab \not\equiv 0$ (3) となることから (3) は素イデアルである。

Sm 3 ○ ガウスの整数環 $\mathbb{Z}[i]$ のイデアル (3) と $(1+i)$ は素イデアルであるが (2) は素イデアルでない

[証明] $a + bi = 3(c + di) + a' + b'i$ $(0 \leq a', b' < 3)$
で $0 \leq a, b, a', b' < 3$ なる $a \not\equiv a'$ or $b \not\equiv b'$ に於て $a' + b'i \not\equiv a'' + b''i$ (3) であるから この $a' + b'i$ は $\mathbb{Z}[i]/(3)$ を代表する。

$a'+b'i \neq 0$ の積をとると $1(a+bi)=-b+ai$, $a(c+di)=ac+adi$
$(1+i)^2=2i$, $(1+i)(1+2i)=-1+3i$, $(1+i)(2+i)=1+3i$
$(1+i)(2+2i)=4i$, $(1+2i)^2=-3+4i$, $(1+2i)(2+i)=5i$
$(1+2i)(2+2i)=-2+6i$, $(2+i)^2=3+4i$, $(2+2i)^2=8i$
$(2+i)(2+2i)=2+6i$ でどれも $\alpha \neq 0$, $\beta \neq 0$ に対して
$\alpha\beta \neq 0$ (3) である。よって (3) は素イデアルである。
$a+bi=2(c+di)+a'+b'i$ $(0 \leq a', b' < 2)$ であるが ところが
$2=(1+i)(1-i)$ であるから $1+i$ の剰余類は 上の $a'+b'i$ について
調べれば充分である。これらは $1, i, 0, 1+i$ からなるが $1+i$ は 0 と
同じ剰余類に属すから, $1, i, 0$ について調べれば十分である。
この3つの要素のうち 0 でない要素 $1, i$ の積 $1^2, i^2, 1\cdot i$ はいずれも
$(1+i)$ に属さないから $(1+i)$ は素イデアルである。最後に (2) は (2)
に属さない要素 $1+i$, $1-i$ の積が (2) に属すから素イデアルでは
ない。

▷ 最大公約イデアル … 2つのイデアル $\mathfrak{a}, \mathfrak{b}$ の合併集合から生成されるイデアル $(\mathfrak{a}, \mathfrak{b})$ のことをいう。すべての公約イデアルで割りきれる。
最大公約イデアル
$(\mathfrak{a}, \mathfrak{b})$ は $a \in \mathfrak{a}$, $b \in \mathfrak{b}$ の $a+b$ 全体からなるので $\mathfrak{a}, \mathfrak{b}$ の和ともいう。
和

最小公倍イデアル … 2つのイデアル $\mathfrak{a}, \mathfrak{b}$ の共通集合 $\mathfrak{a} \cap \mathfrak{b}$ のことをいう。すべての公倍イデアルを割りきる。
最小公倍イデアル

§18. ユークリッド環と単項イデアル環

▷ ユークリッド環
ユークリッド環
○ 可換環 R の 0 と異なる要素 (R は零以外の要素をもっていると仮定している) a に, 負でない整数 $g(a)$ が対応させられている。

1. $a \neq 0$, $b \neq 0$ に対して, $ab \neq 0$ で, $g(ab) \geq g(a)$
2. (割り算) 環の2つの要素 a, b $(a \neq 0)$ に対して
$$b = \delta a + \gamma$$
という表示が成り立ち。$\gamma = 0$ か, $g(\gamma) < g(a)$ である。

○ ユークリッド環に於ては, すべてのイデアルが単項である。
[証明] $g(a)$ が最小になるイデアル $\mathfrak{n}$ の要素の1つ a をとる。イデアル $\mathfrak{n}$ の任意の要素 b は $b=\delta a+\gamma$, $g(\gamma) < g(a)$ 又は $\gamma = 0$

第3章 第18節

と表わされる $b-\beta a$ 即ち r は明らかに $\mathfrak{n}$ に属する。よって $g(r) \geqq g(a)$ でなくてはならない。これと $r=0$ 又は $g(r)<g(a)$ から $r=0$ を得る。よって イデアル $\mathfrak{n}$ の任意の要素 b は a の 倍元となり，それは単項イデアルである。

- $R=\mathbb{Z}$ の時は $g(a)=|a|$ とおく。
  $R=K[x]$（体 K 上の多項式環）の場合は $g(a)=\deg a$

単項イデアル環

- 単位要素を含む整域で，すべてのイデアルが単項イデアルである時，この整域を単項イデアル環という。

- ユークリッド環は単位要素 e をもつ。（∵単位イデアルが単項であるから (a) となるが特に $a=ae$ ともなるから $b=a\beta$ に対し $eb=ea\beta=a\beta=b$ ）
- ユークリッド環では 単項イデアルでは，どの2要素も最大公約元をもち，それは $d=ra+sb$ の形に表わせる。

▷ 最大公約元を $d=(a,b)$ と表わす。（正確には (d) がきまるのだから $(d)=(a,b)$ と書くべきだが，ここでは慣用の記法を使う）

因子無縁
互いに素

a,b は因子無縁あるいは互いに素 …… $(a,b)=1$

▷ ユークリッドの互除法 （環はもちろんユークリッド環である）

ユークリッドの互除法

環の2つの要素 a_0, a_1 が与えられ 例えば，$g(a_1) \leqq g(a_0)$ とする。
次の割り算を順次行なう。

$$a_0=\beta_1 a_1+a_2 \qquad g(a_2)<g(a_1)$$
$$a_1=\beta_1 a_2+a_3 \qquad g(a_3)<g(a_2)$$
$$\cdots\cdots \qquad \cdots\cdots$$
$$a_{s-1}=\beta_{s-1} a_s$$

この時すべての数 $a_0, a_1, \cdots, a_s$ が ra_0+sa_1 の形をしている。a_s の任意の約元（a_s 自身も）は a_{s-1} の約元で 従って a_{s-2} の約元で …… a_1, a_0 の約元である。だから a_s は a_0 と a_1 との最大公約元である。 $a_s=(a_0,a_1)$

▷ 可換である環では 条件

$$b=\beta_1 a+r_1=a\beta_2+r_2 \quad , \quad g(r_1)<g(a) \quad , \quad g(r_2)<g(a)$$

を満足する $\beta_1, \beta_2, r_1, r_2$ の存在を仮定する。

この時可換の場合と同様にして右イデアルは a の右倍元全体に，左イデアルは a の左倍元全体に，両側イデアルは a の右倍元にも左倍元にもなっている。特にこれを単位イデアルに適応すると，前と同様に単位元の存在が導ける。更に，2つの要素 a, b の左側最大公約元，右側最大公約元の存在も証明される。

Sm 1 ◦ $(a, b) = d$ という関係は，環 R を R を含むかってな環に拡大しても変わらない。（但し両方ともユークリッド環である）

［証明］ d の必要にして十分な条件

$$d = \gamma a + \delta b, \quad a = \varepsilon d, \quad b = \eta d$$

は R を含む環 R' に於ても成り立つから d は R' でも $a \cdot b$ の最大公約元とる。

Sm 2 ◦ ユークリッド環に於ては，逆要素 ε^{-1} をもつ要素 ε は，$g(\varepsilon) = g(1)$ という条件で特徴づけられる。

［証明］ $\varepsilon \neq 0$, $\varepsilon^{-1} \neq 0$ であるから $g(\varepsilon \cdot \varepsilon^{-1}) \geqq g(\varepsilon)$

即ち $g(1) \geqq g(\varepsilon)$，ところが $g(\varepsilon) = g(1 \cdot \varepsilon) \geqq g(1)$ 故に $g(1) = g(\varepsilon)$，逆に $g(1) = g(\varepsilon)$ とする。$1 = \beta \cdot \varepsilon + \gamma$, $g(\gamma) < g(\varepsilon)$ 又は $\gamma = 0$ とする。もし $\gamma \neq 0$ ならば $g(\gamma) < g(\varepsilon)$ 故に $g(\gamma) < g(1)$ ところが $g(\gamma) = g(\gamma \cdot 1) \geqq g(1)$ であるから不合理。よって $\gamma = 0$ 即ち $1 = \beta\varepsilon$ なる β が存在する。

Sm 3 ◦ 2つの整数 r, s が互いに素る時，即ち $(r, s) = 1$ の時 群 G の位数 $r \cdot s$ の要素 a は，一意的にきまった位数 s の要素 $a^{\lambda r}$ と一意的にきまった位数 r の要素 $a^{\mu s}$ との積になる。

［証明］ $(r, s) = 1$ より $1 = \lambda r + \mu s$ なる λ, μ が存在する，この λ, μ をとれば $a^{\lambda r} a^{\mu s} = a$ であることは容易にわかる。他の $1 = \alpha r + \beta s$ に対して $a^{\lambda r} = a^{\alpha r}$, $a^{\mu s} = a^{\beta s}$ であることを証明する。

要素 $a^{(\lambda - \alpha) r}$ を ρ, $a^{(\beta - \mu) s}$ を δ とすると $\lambda, \mu, \alpha, \beta$ の定義から $\rho = \delta$ である。ρ は位数 s をもつ要素同士の積であるから $\rho^s = e$

同様に δ は $\delta^r = e$; $\rho = \delta$ であるから $\rho^s = e$, $\rho^r = e$, $\lambda r + \mu s = 1$ だから $\rho = \rho^{\lambda r + \mu s} = \rho^{r\lambda} \cdot \rho^{s\mu} = e = \delta$ よって $a^{(\lambda - \alpha) r} = e$ 即ち $a^{\lambda r} = a^{\alpha r}$, $a^{(\beta - \mu) s} = e$ より $a^{\beta s} = a^{\mu s}$

Sm 4 ◦ 要素 a から生成される位数 n の巡回群では，a^{μ}, $(\mu, n) = 1$ の形の要素はすべて生成要素である。

［証明］ $(\mu, n) = 1$ より $1 = \alpha\mu + \beta n$ とる。$a^{\alpha\mu} = a^{1 - \beta n} = a$ であるから a^{μ} は $\{a\}$ を生成する。もちろん $\{a^{\mu}\} \subseteq \{a\}$ である。

第3章 第18節

▷ ガウスの整数環 $\mathbb{Z}[i]$ の割り算

ノルム $g(a+bi) = a^2+b^2$ この g を $N(a+bi)$ と表わし <ノルム> という。

等式 $N(\alpha\beta) = N(\alpha)N(\beta)$ が成り立つ。

$N(a+bi) = a^2+b^2$ であるから $a+bi \neq 0$ で $N(a+bi) > 0$, $N(0) = 0$

○ ガウスの整数環 $\mathbb{Z}[i]$ は整域である。

$\alpha \neq 0$, $\beta \neq 0$ とすれば $N(\alpha\beta) = N(\alpha)N(\beta) > 0$ 従って $\alpha\beta \neq 0$

これから $\mathbb{Z}[i]$ には商体が存在する。 $\alpha = a+bi \neq 0$ なるは

$\alpha^{-1} = \frac{a-bi}{N(\alpha)}$ である。従って商体の数は $\frac{a}{n} + \frac{b}{n}i$ (a, b, n は有理整数)

の形で表わされる。これらの分数が集って ガウスの数体 $P(i)$ をなす。

ノルムの定義と $N(\alpha\beta) = N(\alpha)N(\beta)$ はこの体にも正しい。

○ α, $\beta \neq 0$ に対して $P(i)$ の中で $\alpha - \lambda'\beta = 0$ を解く。

この $\lambda' = a'+b'i$ をまめ それから, a', b' の代りに, これにもっとも近い整数 a b をえれて, $\lambda = a+bi$, $\lambda' - \lambda = \varepsilon$ とおく。すると

$$\alpha - \lambda\beta = \alpha - \lambda'\beta + \varepsilon\beta = \varepsilon\beta$$

$$N(\alpha - \lambda\beta) = N(\varepsilon)N(\beta)$$

$$N(\varepsilon) = N(\lambda' - \lambda) = (a'-a)^2 + (b'-b)^2 \leqq \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 < 1$$

$$N(\alpha - \lambda\beta) < N(\beta)$$

となる 従って

$$\alpha = \lambda\beta + \gamma \qquad (\ N(\gamma) < N(\beta)\ )$$

なる γ が存在する。(割り算可能)

Sm 5 ○ 数 $a+b\rho$ から成る環 $\mathbb{Z}[\rho]$ を, 1, ρ を基底にもつ有理整数環 $\mathbb{Z}$ 上の2元環と考えて割り算を行なう。但し $\rho^2 = -\rho - 1$

[証明] $N(a+b\rho) = a^2 - ab + b^2$ とすると。

$N(\alpha\beta) = N(\alpha)N(\beta)$ が成り立つ。特に $\alpha \neq 0$ の時 $N(\alpha) > 0$, $N(0) = 0$

$a+b\rho$ は先の $\mathbb{Z}[i]$ と同様に整域である。よってその商体 $P[\rho]$ がつくられる。 $\alpha = a+bi$ の時 $\alpha^{-1} = (a+bi)^{-1} = \frac{a-b-b\rho}{N(\alpha)}$ となり $P[\rho]$ は $\frac{a}{n} + \frac{b}{n}\rho$ なる数から成る。 $\alpha - \lambda'\beta = 0$, $(\beta \neq 0)$ を $P[\rho]$ で解きその $\lambda' = a'+b'\rho$ にもっとも近い整数に a', b' をかえて $\lambda = a+b\rho$ をつくる。この時 $\lambda' - \lambda = \varepsilon$ とおく。 $N(\alpha - \lambda\beta) = N(\alpha - \lambda'\beta + \varepsilon\beta)$

$= N(\varepsilon\beta) = N(\varepsilon)N(\beta)$

$$N(\varepsilon) = (a'-a)^2 - (a'-a)(b'-b) + (b'-b)^2 = \frac{1}{4}(2\bar{a} - \bar{b})^2 + \frac{3}{4}\bar{b}^2$$

$|2\bar{a} - \bar{b}| \leqq 2|\bar{a}| + |\bar{b}| \leqq \frac{3}{2}$ $\therefore N(\varepsilon) \leqq \frac{9}{16} + \frac{3}{16} < 1$

$\therefore\ N(\alpha-\lambda\beta) < N(\beta)$　即ち割り算が可能である。

Sm.6 ◦ Sm.5と同様にして 数 $a+b\sqrt{2}$ の環 $\mathbb{Z}[\sqrt{2}]$ や 数 $a+b\sqrt{-2}$ の環 $\mathbb{Z}[\sqrt{-2}]$ の割り算が可能である。 $a+b\sqrt{-3}$ の環 $\mathbb{Z}[\sqrt{-3}]$ や $a+b\sqrt{-5}$ の環 $\mathbb{Z}[\sqrt{-5}]$ の場合に，この方法は役に立たない。イデアル $(2, 1+\sqrt{-3})$ は Sm5にあげた環において単項である。

[証明] $N(\alpha\beta)=N(\alpha)N(\beta)$ が成り立つように $N(\alpha)$ を定義する。

$N(a^2-2b^2)=N(a+b\sqrt{2})N(a-b\sqrt{2})$，整数 a に対して $N(a)=a^2$ と定義すると $(a^2-2b^2)^2 = N(a+b\sqrt{2})N(a-b\sqrt{2})$

$\therefore\ N(a+b\sqrt{2}) = a^2-2b^2$ とおけばよい。 すると

$N(\alpha\beta)=N(\alpha)N(\beta)$ が成り立つ。

$\alpha\neq 0$ の時 $N(\alpha)\neq 0$， $N(0)=0$ 故に前と同様に商体 $P[\sqrt{2}]$ を導入する。前と同様に数を選べば

$N(\alpha-\lambda\beta)=N(\varepsilon)N(\beta)$ とおり

$N(\varepsilon)=|\bar{a}^2-2\bar{b}^2| < 1$

$|N(\alpha-\lambda\beta)| < |N(\beta)|$ となる。

$\mathbb{Z}[\sqrt{-2}]$ の $a+\sqrt{-2}b$ の $N(a+\sqrt{-2}b)$ を a^2+2b^2 とする

こうすると $N(\alpha\beta)=N(\alpha)N(\beta)$ が成り立つ。$\alpha\neq 0$ の時 $N(\alpha)\neq 0$.

だから前と同様に $P[\sqrt{-2}]$ を作り同様に数を選べば

$N(\alpha-\lambda\beta)=N(\varepsilon)N(\beta)$

$N(\varepsilon) = \bar{a}^2+2\bar{b}^2 < 1$

で $N(\alpha-\lambda\beta) < N(\beta)$ となる。

$\mathbb{Z}[\sqrt{-3}]$ では $N(a+\sqrt{-3}b)=a^2+3b^2$ であるがやはり前と同様に $N(\varepsilon)$ を調べると $N(\varepsilon)=\bar{a}^2+3\bar{b}^2 \leq 1$ となってしまい。割り算はこの方法では可能とはならない。$\sqrt{-5}$ も同様である。

$(2, 1+\sqrt{-3}) = (2, 2\rho+1)$ はもちろんの単項である。

$2\rho+1 = 2\cdot\rho+1$　　$N(1)<N(2)$

$2 = 1\cdot 2$

従って最大公約元 d は 1 である。実際この時 $2\rho+1=(2\rho+1)1$

$2=1\cdot 2$ で 更に $1=(2\rho+1)\cdot 1+2\cdot(-\rho)$ となる。従って イデアル $(2, 1+\sqrt{-3})$ は単位イデアル (1) と一致する。

第3章 第19節

§19 素因子分解

▷ この節では単位要素をも整域について述べている。

単元
- 単元（正則要素） … 整域内（もちろん単位要素はもつ）に逆要素 ε^{-1} をもつ要素 ε のこと。（ε^{-1} も単元となる）

自明な分解
- 自明な分解 $a = a\varepsilon^{-1}\cdot\varepsilon$ （ε は単元）

素元
- 素元（既約要素） …… $p\neq 0$ に対して $p=ab$ ならば 必ず a か b か一方が単元である。（多項式の時は既約多項式，整数の時は素数（>1））

同伴
- 同伴な2要素 …… a, $b=a\varepsilon^{-1}$ （ε は単元） なる a, b

この時 イデアル $(a)=(b)$ である。逆に $(a)=(b)$ ならば a, b は同伴である。

真の約元
- 真の約元 …… $a=cd$ で d が単元でないような c，この時 $(a)\subset(c)$ である。

注）素元を $p\neq 0$ で真の約元をもたない要素といってもよい。

▷ ユークリッド環では，b が a の真の約元であれば $g(b)<g(a)$ が成り立つ。

［証明］ $(a)\subset(b)$ であるから $b=a\beta+r$ と書いた時 $r\neq 0$ である。$a=bc$ （c は単元ではない）であるから $r=b-a\beta=b(1-c\beta)$ これから $g(r)\geq g(b)$，が成り立つ。先の式から $g(r)<g(a)$ であるから結局 $g(b)<g(a)$

▷ ユークリッド環では，0と思えるすべての要素 a が素元の積になる。

［証明］ $g(p)=0$ の時は もし p に真の約元があれば $g(\beta)<0$ となり不合理となる（$g(\alpha)\geq 0$）からこのような p は素元である。従って $g(p)=0$ に対しては定理は成り立つ。$g(u)<n$ なる u に対して定理が成り立つとする。$g(v)=n$ に対して，もし v が素元なら問題はない。従って v は素元でないとする，すると $v=cb$ なる真の約元 c が存在する。$g(c)<g(v)$ である。同様に c は単位要素ではないとれるから，b についても $g(b)<g(v)$ となり c, b については定理は成り立つから v についても証明された。

▷ 単項イデアル環では，単元でない素元は極大素イデアルを生成する。

［証明］ p が素元であるから単元以外真の約元をもたない。従ってイデアル (p) は単位イデアル以外の約イデアルをもたない。（∵ イデアルはすべて単項であるから）

○ 積が素元 p で割りきれれば，その因子の1つも p で割りきらなければならない。（剰余環 $R/(p)$ が体であるから零元をもたない）

Sm. 1 ○ 合同式 $6x \equiv 7\ (19)$ を満たす x を求めよ。

［解答］ (19) に属さない要素 6 と 19 の生成するイデアルは単位イデアルになる（(19) が極大である）よって $1 = 6\gamma + 19s$ なる γ, s が存在する。実際に $1 = 6(-3) + 19\cdot 1$ である。両辺に 7 を乗じて合同式になおすと。 $6(-21) \equiv 7\ (19)$，$-21 \equiv -2\ (19)$ だから。$6(-2) \equiv 7\ (19)$，ここで剰余環 $R/(19)$ は体であるのだから除法の一意性が成り立ち結局 $x \equiv -2\ (19)$ なる x が解となる。

Sm. 2 ○ (19) を法とする整数の剰余体に於て，6 の剰余類の逆要素は何か。

［解答］ 合同式 $6x \equiv 1\ (19)$ を解けばよい。（剰余体では $\overline{6}\,\overline{x} = \overline{1}$）前と同様に $1 = 6(-3) + 19\cdot 1$ であるから これを合同式になおして $6(-3) \equiv 1\ (19)$，（剰余体では $\overline{6}\,\overline{(-3)} = \overline{1}$）即ち -3 の属する剰余類である。

▷ 素因子分解

素因子分解の一意性 …… 単項イデアル環で $a = p_1 p_2 \cdots p_r$ と $a = q_1 \cdots q_s$ を同一数 a の2つの分解とする。a が単元で従って p_i も q_j も皆単元である（∵ $\varepsilon = p_1 p_2 \cdots p_r$ だと $\varepsilon\varepsilon^{-1} = p_1 \cdots p_r \varepsilon^{-1} = 1$ となり $p_i\ (i = 1, 2, \cdots, r)$ は単元となる）更に因子 p_i，q_j のうちに単元があれば，それらはすべて因子 p_u，q_v（p_u，p_v は単元ではない）の中にくみ込まれてしまったと仮定してよい。だからすべての，p_i，p_j は単元ではない。すると次のことが成立する。

○ $r = s$ で順序の違いを別にし，単元因子の違いを別にすれば，p_i は q_j に一致する。

［証明］ $r = 1$ の時は定理は明白。$r < n$ に対して定理が成り立つとする。 $p_1 \cdots p_n = q_1 \cdots q_m$ であるから 積 $q_1 \cdots q_m$ は p_1 で割りきれるから 因し q_i のうち1つが p_1 で割りきれる。q_i と q_1 の番号をつけかえて q_1 が p_1 で割りきれるようにする。つまり $q_1 = \varepsilon_1 p_1$（ε_1 は明らかに単元となる）これをもとの式に代入して簡約すれば

$$p_2 \cdots p_n = (\varepsilon_1 q_2) \cdots q_m$$

帰納法の仮定よりこの両辺の因子は，単元の違いを別にして一致する。結局 $p_1 \cdots p_n = q_1 \cdots q_m$ にもこれによって定理が成り立つ。

第3章 第19節

Sm. 3 ◦ 有理整係数の多項式 $f(x)$ は，任意の素数 p を法として，p を法とする既約な因子にただ1通りに分解される。

［証明］ 有理整係数の多項式 $f(x)$，$g(x)$ につき

$f(x) \equiv g(x) + r \quad (p)$，　$\deg r < \deg g(x)$ または $r = 0$

が成り立てば $f(x), g(x) \in \mathbb{Z}[x]$ の剰余環 $\mathbb{Z}[x]/(p)$ がユークリッド環となり その単元の違いを除いて $\mathbb{Z}[x]/(p)$ 内で $f(x)$ が一意的に因数分解されるはずである。

$f(x)$ の最高次の係数を a とする。 $px^k \equiv 0 \ (p)$ であるから $g(x)$ の属する剰余類の中には最高次の係数が (p) に属さぬものがある。（$g(x) \not\equiv 0 \ (p)$ を使っている）剰余類の代表としてそのような $g'(x)$ をとると $g'(x) = b_0 x^m + \cdots + b_m$ （$b_0 \not\equiv 0$）。次に 方程式 $a \equiv b_0 u \ (p)$ をとく。もし $\deg f(x) < \deg g'(x)$ なるは r としてそのまま $f(x)$ をとればよいから $\deg f(x) \geqq \deg g'(x)$ とする。

この時 $q = u x^{n-m}$，（但し $n = \deg f(x)$，$m = \deg g'(x)$）とおくすると。 $ax^n + \cdots + c = u x^{n-m}(b_0 x^m + \cdots + b_m) + r \quad (p)$

となり $\deg r \leqq n-1$ となる。次に 同様のことを $f(x)$ の代わりに r について行ない $r_1, r_2, \cdots$ と順次次数を下げていく そしてついには $\deg r_s < \deg g(x)$ となり上の表示が得られる。

Sm. 4 ◦ ガウスの整数環の単元は何か。この環内で 2, 3, 5 はどのように因数分解されるか。

［解答］ 0 はあらかじめ除外しておく。（0は逆要素をもたない。）

もし $\varepsilon = a+bi$ に逆要素が存在すればそれを $\varepsilon^{-1} = c+di$ とおく。

$N(a+bi)\,N(c+di) = N(\varepsilon)N(\varepsilon^{-1}) = N(1) = 1$

$\therefore \quad (a^2+b^2)(c^2+d^2) = 1$

a, b, 共に0となることはないから $a^2+b^2 \geqq 1$，同様に $c^2+d^2 \geqq 1$ よって $a^2+b^2 = 1$，よって $a \neq 0$ なるは $a^2 \geqq 1$ であるから $b=0$ $\therefore \ a = \pm 1$

$a=0$ なるは $b = \pm 1$ 従って単元になるのは $1, -1, i, -i$ の中に入るければなるない。とこうが $1 \cdot 1 = 1$，$(-1)(-1) = 1$，$i(-i) = 1$ だからこれらは単元である。よって $\mathbb{Z}[i]$ の単元は $\pm 1, \pm i$ である。

$2 = (1+i)(1-i)$ であるが $1+i$ と $1-i$ は素元である。もしこれが素元でなければ $\eta < N(1+i) = 2$ なる単元でない負の約元が定まるが，$\eta \neq 0$ であるから $0 < \eta$ で よって $N(\eta) = N(1)$，前節 Sm. 2 によって η は単元となる。従って $1+i$，$1-i$ は共に素元である。（$1-i$ も同様）

3が因子に分解されたとする。 $3 = (a+bi)(c+di)$ 先のことから3が素元でないとすると $N(a+bi)$，$N(c+di) \neq 1$ としてよい。

$N(3)=N(a+bi)N(c+di)$ $\therefore$ $(a^2+b^2)(c^2+d^2)=9$

整数9の$\mathbb{Z}$における分解は $1\cdot9$, $9\cdot1$, $3\cdot3$ だが $N(a+bi)\neq1$ $N(c+di)\neq1$ だから $a^2+b^2=3$ で $c^2+d^2=3$ である。

$a^2<4$ $\therefore$ $a<2$ $\therefore$ $a=0,1$ よって $a=0$ とすると $b^2=3$ となる。$1^2=1$, $2^2=4$ であるからこのような b はない。$a=1$ とすると $b^2=2$ となるが同様にこのような b も存在しない。よって3は素元である。

$5=(1+2i)(1-2i)$ となるが もし $1+2i$ ($\mathbb{Z}$は $1-2i$) が素元でなければ数 α が存在し $N(\alpha)\neq1$ で 上と同様に $N(\alpha)$ が $N(1+2i)=5$ の1真の約元となる。5の真の約元は1だけだから このような α は存在しない。

Sn. 5 ◦ 数 $a+b\sqrt{-3}$ の環 $\mathbb{Z}[\sqrt{-3}]$ において数4は本質的に異なった2つの素因子分解 $4=2\cdot2=(1+\sqrt{-3})(1-\sqrt{-3})$ をもつ。

[証明] 2が素元であることを証明する。もし2が素元でなければ $N(2)$ の1でない真の約数を $N(\alpha)$ にもつ α が存在する。$N(2)=4$ であるから $N(\alpha)$ は2でなければならない。ところが $a^2+3b^2=2$ を満たす整数 a, b は存在しない。$\because$ $b\neq0$ ならば $3b^2\geq3$ であるから $b=0$, 従って $a^2=2$ となる。このような a は存在しない。$1+\sqrt{-3}$, $1-\sqrt{-3}$ も又 $N(1+\sqrt{-3})=4$ をもつから同様に素元である。従ってこの2つが同伴でないことを証明すればよい。$N(1)=1$ だから 単元 ε に対して $N(\varepsilon)=1$ である。$a^2+3b^2=1$ なる a,b は, $a=\pm1$, $b=0$ のみであるから単元は ±1 である。しかるに 2にそれらを乗じても $1+\sqrt{-3}$, $1-\sqrt{-3}$ とならないから, この素因子分解は本質的に違っている。

Sn. 6 ◦ 単項イデアル環においては, 法 a の剰余類で a と互いに素な要素からなるものは, 乗法に関して群をつくる。

[証明] β,γ が同じ剰余類に属するとき その差 $\beta-\gamma$ は (a) に属する。

β と a のつくるイデアル (β,a) と (γ,a) は等しい。なぜなら

$(\beta,a)=(\beta+a\gamma,a)\subseteq(\gamma,a)$ 同様に $(\gamma,a)\subseteq(\beta,a)$ で $(\beta,a)=(\gamma,a)$ よって β と a が素なとき $\bar{\beta}$ に属する要素と a は素で素でないものすべては素ではない。剰余類 $\beta\in\bar{\beta}$ と $\gamma\in\bar{\gamma}$ が a に対して共に素であれば $\beta\gamma$ は a に対して素である。($\because u_1\beta+u_2a=1$, $v_1\gamma+v_2a=1$ だから両方を乗じて $u_1v_1\beta\gamma+(u_1v_2+v_1u_2+u_2v_2a)a=1$ 即ち $(\beta\gamma,a)=1$) よって $\bar{\beta}\bar{\gamma}$ の要素はすべて a に素である。問題の剰余類の集合を H とすると, $\bar{\beta}\in H$, $\bar{\gamma}\in H$ に対して今のことから $\bar{\beta}\bar{\gamma}\in H$ 次に $(1,a)=1$ だから $\bar{1}$ は H に属し $\bar{1}\bar{\beta}=\bar{\beta}$ である。更に $\bar{\beta}\in H$ の $\bar{\beta}$ の1つの要素 β につき $u\beta+va=1$ なる u,v が存在するからこれを剰余類にうつすと $\bar{u}\bar{\beta}=\bar{1}$ となる $\bar{u}$ が存在する。よって H は群である。

第8章第19節

▷ ◦ Rにおいて，すべての要素がただ1通りに素因子に分解されるならば，素元は素イデアルを生成し，0以外の可約な要素が生成するイデアルは，素ではない。

［証明］ pは素元であるとする。$ab \equiv 0\ (p)$ とすると ab の素因子分解には，pが因子としてでてこなければならない。ところが，ab の素因子分解は a と b の素因子分解を合わせたものだから，a, b どちらか少なくても一方の素因子分解の中にpがある。よって $a \equiv 0\ (p)$ か $b \equiv 0\ (p)$
次にpを素元でないとし $p = a \cdot b$ とする。 a, b はpの真の約元とすると $ab \equiv 0\ (p)$，$a \not\equiv 0\ (p)$ $b \not\equiv 0\ (p)$ 即ち (p) は素ではない。

Sm 7. ◦ 素因子分解の一意性の成り立つ環に於ては，2つあるいはそれ以上の要素に対して ＜最大公約元＞と＜最小公倍元＞が存在し単元の違いを無視すれば一意的にきまる。

［証明］ 2要素 $a = p_1 \cdots p_r$，$b = q_1 \cdots q_s$ の最大公約元 d はそれ自身 a, b の約元で，それに単元でないRのどんな要素を乗じても a, b の約元ではなくなるものとする。 するとまず a, b の最大公約元 d はその素因子の中に $p_1, \cdots p_r$，$q_1, \cdots, q_s$ 以外を含んではならない。（d は ab の約元となるから） a の素因子 $p_1, p_2, \cdots, p_r$ のうち b にも含むもの（もし同じ $p_i, p_k \cdots$（m 個）があれば b にある個数と m の低い方をとって1個ずつ素因子の列に列挙して $p_{\alpha_1}, p_{\alpha_2}, \cdots, p_{\alpha_n}$ を作る。d は a のこれ以外の要素を含んではならない。これ以外の要素を含むと b の約元とならない。そこに $d' = p_{\alpha_1} \cdots p_{\alpha_n}$ は確かに a, b 両方の約元になっている。もしこれに b の素因子 p を乗じるとそれは a になるかまたはその素因子の pd' に表れるpの個数が a のそれをこえるから a の約元にはならない。従って d' は a, b の最大公約元 d に等しい。要素が3以上の時も同様に行えばよい。最小公倍元は a, b 両方の倍元でその真の約元がどれも a, b 両方の倍元にならないものと定義する。
これとはその要素として a, b 両方にあらわれる素因子すべての積（それぞれの個数も考りょに入れて）と定義すればこれがその条件を満たすことがわかる。 3個以上の時も同様。

注） Sm.7で定義した最大公約元のイデアルは必ずしも最大公約イデアルとはならない。例として $\mathfrak{Z}[\alpha]$ の2つの要素 2と α を考えれば $\mathfrak{Z}[\alpha]$ は次章で証明する通り素因子分解の一意性が成り立ち上の意味での2と α の最大公約元は1で(1)は $(2, \alpha)$ と一致しない。

第4章　有理整函数

§20　微分

▷ 微分

微分

○ 多項式環 $R[x]$，（Rは可換以後特に断わるなり限りこの章では環は可換とする）多項式環 $R[x,h]$ で 多項式 $f(x+h)$；$(f(x)\in R)$ $=\sum a_i(x+h)^i$ を作りこれをhのべきに展開すると

$$f(x+h)=f(x)+hf_1(x)+h^2f_2(x)+\cdots$$

又は　$f(x+h)\equiv f(x)+hf_1(x)\pmod{h^2}$

この $f_1(x)$ を（$f(x)$によって一意的にきまる）を $f(x)$ の導函数といい $f'(x)$ で表わす。$f'(x)$ を得るには $f(x+h)-f(x)$ を作りそれをhで割って $h=0$ とすればよい。この定義はRが実数体等の時の導函数の定義と一致する。よって $f'(x)$ を

導函数

$$\frac{df}{dx}\quad\text{あるいは}\quad\frac{d}{dx}f(x)\qquad(1)$$

と表わしてもよい。もとの多項式環が $R[x_1,x_2,\cdots,x_n]$　$n\geq 2$ の時は(1)の代わりに

$$\frac{\partial f}{\partial x},\qquad\frac{\partial}{\partial x}f(x),\qquad f_x$$

等と表わす。

Ⅰ　加法公式　$(f+g)'=f'+g'$

Ⅱ　乗法公式　$(fg)'=f'g+fg'$

Ⅲ　連加公式　$(f_1+f_2+\cdots+f_m)'=f_1'+f_2'+\cdots+f_m'$

Ⅳ　連乗公式　$(f_1\cdots f_n)'=f_1'f_2\cdots f_n+f_1f_2'f_3\cdots f_n+\cdots+f_1f_2\cdots f_n'$

Ⅴ　べキの導函数　$(ax^m)'=max^{m-1}$

Ⅵ　$f(x)=\sum_0^n a_ix^i$ の導函数　$f'(x)=\sum_1^n ia_ix^{i-1}$

［証明］Ⅰ　$f(x+h)+g(x+h)\equiv f(x)+g(x)+h(f'(x)+g'(x))$

Ⅱ　$f(x+h)g(x+h)\equiv\{f(x)+hf'(x)\}\{g(x)+hg'(x)\}$

$\equiv f(x)g(x)+h\{f(x)g'(x)+f'(x)g(x)\}$

（$\equiv$ は $\bmod h^2$ について）　Ⅲ Ⅳ Ⅴ Ⅵ はこれらから容易に導けるので省略　上の微分について述べたことは非可環Rでも成り立つ。

第4章 第20節

Sm. 1 ○ $F(\xi_1, \cdots, \xi_m)$ は多項式として $F_\nu = \dfrac{\partial F}{\partial \xi_\nu}$ とおくと 公式

$$\frac{d}{dx} F(f_1(x), \cdots, f_m(x)) = \sum_1^m F_\nu(f_1, \cdots, f_m) \frac{df_\nu}{dx}$$

が成り立つ。

[証明] まず $F(\xi_1, \cdots, \xi_m)$ を単項式とし $F = a f_1^{p_1} f_2^{p_2} \cdots f_m^{p_m}$ (但し f_i は $f_i(x)$ を略記したもの F は $F(x)$ の略) とおく。

すると $F(x+h)$ を見ると

$$F(x+h) \equiv a(f_1 + h f_1')^{p_1}(f_2 + h f_2')^{p_2} \cdots (f_m + h f_m')^{p_m} \pmod{h^2}$$

が成り立つ。 $(f_1 + h f_1')^{p_1}$ を計算する。 $g(y) = y^{p_1}$ とする。

$(y+k)^{p_1} \equiv y^{p_1} + k p_1 y^{p_1-1} \pmod{k^2}$ であるから。

$(f_1 + h f_1')^{p_1} \equiv f_1^{p_1} + h f_1' p_1 f_1^{p_1-1} \pmod{h^2 f_1'^2}$

$\therefore \quad (f_1 + h f_1')^{p_1} \equiv f_1^{p_1} + h f_1' p_1 f_1^{p_1-1} \pmod{h^2}$

$$p_1 f_1^{p_1-1} = \frac{1}{a f_2^{p_2} \cdots f_m^{p_m}} \frac{\partial F}{\partial \xi_1} \qquad (1, 2, 3, \cdots \text{についても同様にして})$$

$$F(x+h) \equiv a \prod_{i=1}^m \left(f_i^{p_i} + \frac{f_i'}{a f_1^{p_1} \cdots f_{i-1}^{p_{i-1}} f_{i+1}^{p_{i+1}} \cdots f_m^{p_m}} \left[\frac{\partial F}{\partial \xi_i}\right]_{\xi_i = f_i} \right)$$

$$\equiv F(x) + h \sum f_i' \left[\frac{\partial F}{\partial \xi_i}\right]_{\xi_i = f_i}$$

$$\therefore \quad F'(x) = \sum_{\nu=1}^m F_\nu(f_1, \cdots, f_m) \frac{df_\nu}{dx}$$

多項式 $F(x) = F_1(x) + F_2(x) + \cdots + F_n(x)$, $F_i(x)$ は単項式について

$$F'(x) = F_1'(x) + F_2'(x) + \cdots + F_n'(x)$$

$$\therefore \quad F_\nu(\xi_1, \cdots, \xi_m) = F_{1\nu}(\xi_1, \cdots, \xi_m) + \cdots + F_{n\nu}(\xi_1, \cdots, \xi_m)$$

故に

$$F'(x) = \sum_{k=1}^n \sum_{\nu=1}^m F_{k\nu} \frac{df_\nu}{dx} = \sum_{\nu=1}^m F_\nu \frac{df_\nu}{dx} \quad (\text{但し } F_\nu \text{ は上の式})$$

Sm. 2 ○ r 次の同次多項式 $f(x_1, \cdots, x_m)$ について等式

$$f(hx_1, \cdots, hx_m) = h^r f(x_1, \cdots, x_m)$$

が成り立つそれから

$$\sum_\nu \frac{\partial f}{\partial x_\nu} x_\nu = r f$$

[証明] 等式の両辺を h の函数とみて導函数をつくると、Sm. 1 より

$$\sum_1^m f_\nu(hx_1, \cdots, hx_m) = r f(x_1, \cdots, x_m) h^{r-1}$$

$h=1$ とすると

$$\sum_{\nu} \frac{\partial f}{\partial x_\nu} x_\nu = \eta f$$

Sm.3 ○ 体に係数をもつ有理分数函数 $\frac{f(x)}{g(x)}$ について，導函数を代数的に定義して，微分の和，積，商に関する公式を導く。

[解答] 積の定理を保存するために

$$\left(\frac{f(x)}{g(x)}\right)' g(x) + \frac{f(x)}{g(x)} g'(x) = f'(x)$$

とおく．すると

$$\left(\frac{f(x)}{g(x)}\right)' = \frac{f'(x)g(x) - f(x)g'(x)}{\{g(x)\}^2}$$

となる。以後本定義はとえないで $f(x)$ を単に f 等とかく。

$P = \frac{f_1}{g_1}$, $Q = \frac{f_2}{g_2}$ (f_1, f_2, g_1, g_2 は多項式)

$$(P+Q)' = \frac{f_1 g_2 + g_1 f_2}{g_1 g_2} = \frac{(f_1' g_2 + f_1 g_2' + g_1' f_2 + g_1 f_2') g_1 g_2 - (f_1 g_2 + g_1 f_2)(g_1' g_2 + g_1 g_2')}{g_1^2 g_2^2}$$

$$= \frac{g_2^2 (f_1' g_1 - f_1 g_1') + g_1^2 (g_2 f_2' - g_2' f_2)}{g_1^2 g_2^2} = \frac{f_1' g_1 - f_1 g_1'}{g_1^2} + \frac{g_2 f_2' - g_2' f_2}{g_2^2}$$

$$= P' + Q'$$

$$(PQ)' = \frac{f_1 f_2}{g_1 g_2} = \frac{(f_1' f_2 + f_1 f_2') g_1 g_2 - (g_1' g_2 + g_1 g_2') f_1 f_2}{g_1^2 g_2^2}$$

$$= \frac{g_1 (g_2 f_1 f_2' - g_2' f_1 f_2) + g_2 (g_1 f_1' f_2 - g_1' f_1 f_2)}{g_1^2 g_2^2}$$

$$= \frac{f_1 g_1 (g_2 f_2' - g_2' f_2)}{g_1^2 g_2^2} + \frac{f_2 g_2 (g_1 f_1' - g_1' f_1)}{g_1^2 g_2^2}$$

$$= PQ' + P'Q$$

$$\left(\frac{P}{Q}\right)' = \frac{f_1}{g_1}\left(\frac{g_2}{f_2}\right)' + \frac{f_1' g_1 - f_1 g_1'}{g_1^2}\left(\frac{g_2}{f_2}\right) = \frac{f_1}{g_1}\frac{f_2 g_2' - f_2' g_2}{f_2^2} + \frac{g_2}{f_2}\frac{f_1' g_1 - f_1 g_1'}{g_1^2}$$

$$= \frac{g_1 f_1 (f_2 g_2' - f_2' g_2) + g_2 f_2 (f_1' g_1 - f_1 g_1')}{g_1^2 f_2^2} = \frac{\frac{f_2}{g_2}\frac{f_1 g_1' - f_1' g_1}{g_1^2} - \frac{f_1}{g_1}\frac{f_2 g_2' - f_2' g_2}{g_2^2}}{\left(\frac{f_2}{g_2}\right)^2}$$

$$= \frac{P'Q - PQ'}{Q^2}$$

第4章 第21節

§21 零点

▷ 零点（根）

零 点

◦ Rは単位要素をもつ整域であるとする。

◦ R[x]の多項式 $f(x)$に，Rの要素 α が $f(\alpha)=0$ となる。 … この値

▷ α が $f(x)$の零点なら $f(x)$は $(x-\alpha)$で割りきれる。

[証明] $f(x)=g(x)(x-\alpha)+\gamma$ （γは定数）

xにαを代入すると $f(\alpha)=\gamma=0$ ∴ $f(x)=g(x)(x-\alpha)$

▷ $\alpha_1,\alpha_2,\cdots,\alpha_k$ が $f(x)$の相異なる零点なら $f(x)$は積 $(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_k)$で割りきれる。

[証明] $k=1$の時は上の定理より成り立つ。 $k=m-1$の時成り立つとすれば $f(x)=(x-\alpha_1)\cdots(x-\alpha_{m-1})g(x)$ とできる。

両辺に $x=\alpha$を代入すれば

$$f(\alpha_m)=(\alpha_m-\alpha_1)\cdots(\alpha_m-\alpha_{m-1})g(\alpha_m)=0$$

$\alpha_m-\alpha_i$ $(i=1,\cdots,m-1)$ は0に等しくない。Rは整域であるから $g(\alpha_m)=0$ となる。上の定理より $g(x)=(x-\alpha_m)p(x)$

従って $f(x)=(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_m)p(x)$ となる。

▷ 0と異なるn次多項式は，整域内に高々n個の零点しかもたない。

[証明] n個より多い零点をもつとR[x]の多項式 $f(x)$は上の定理からn+1次以上の多項式を因数に含むことになる。このようなことはありえない。

k位の零点

◦ k位の零点 $f(x)=(x-\alpha)^k p(x)$ … αのこと。

$f(x)$のk位の零点は，導函数 $f'(x)$の少なくとも $k-1$ 位の零点である。

[証明] $f(x)=(x-\alpha)^k p(x)$ だから

$$f'(x)=k(x-\alpha)^{k-1}p(x)+(x-\alpha)^k p(x)$$
$$=(x-\alpha)^{k-1}s(x)$$

注） $f(x)=(x-\alpha)p(x)$で $p(\alpha)\neq 0$ ならば

$f'(x)=(x-\alpha)p'(x)+p(x)$ で $f'(\alpha)\neq 0$ である。

▷ $f(x_1,x_2,\cdots,x_m)$ は0と異なる多項式で，不定元 $x_1,x_2,\cdots,x_m$ のおのおのに，R又はRを含む整域の無限個の値を与えることができるとするこの時 その中に $f(\alpha_1,\alpha_2,\cdots,\alpha_m)\neq 0$ をみたす 値の組が 必ず1つは存在する。

［証明］ $f(x_1,\cdots,x_m)$ を 整域 $R[x_1,\cdots,x_{m-1}]$ の x_m の多項式と考えるとそれは高々有限個の零点しか有しない。従って $x_m=\alpha_m$ で $f(x_1,\cdots,x_{m-1},\alpha_m)\neq 0$ なる α_m が存在する。同様にして $x_{m-1}=\alpha_{m-1}$ $x_{m-2}=\alpha_{m-2}$, $\cdots$, $x_1=\alpha_1$ なる1組の R の値を得る。この時 $f(\alpha_1,\alpha_2,\alpha_3,\cdots,\alpha_m)\neq 0$ である。

○ 上の定理を言いかえれば，多項式 $f(x_1,x_2,\cdots,x_m)$ が，無限整域のすべての値に対して0なるは 多項式 $f(x_1,\cdots,x_m)$ は恒等的に0に等しい。

Sm

○ 有限個の多項式 $f_i(x_1,\cdots,x_m)$ が，そのうちどの1つも恒等的に0に等してるいとする時，無限整域の適当なる値 $\alpha_1,\alpha_2,\cdots,\alpha_m$ をとればそれぞれ f_i がみな $f_i\neq 0$ とる。

［証明］ 積 $f_1f_2\cdots f_r$ をつくるとそれはやはり $R[x_1,\cdots,x_m]$ の多項式 F である。先の定理より $F(\alpha_1,\alpha_2,\cdots,\alpha_m)\neq 0$ の $\alpha_1,\alpha_2,\alpha_3\cdots,\alpha_m$ が存在する。この時 明らかに $f_i(\alpha_1,\alpha_2,\cdots,\alpha_m)\neq 0$ $(i=1,\cdots,r)$ とる。

§ 22 補間公式

▷ この節の多項式は1元であるとする。但し係数域は体であるとする。

補間公式

次数 $\leqq n$ の2つの多項式が $n+1$ 個の点で同一の値となれば その2つは同じ多項式である。従って 相異なる点 $\alpha_0,\alpha_1,\cdots,\alpha_n$ で与えられた値 $f(\alpha_i)$ をとる多項式は，存在しても高々1つである。下記より又 必ず1つは存在することがわかる。 （ それぞれの式はこのような性質をもつ式である。→ $f(x)$ ）

▷ ラグランジュの補間公式

ラグランジュの補間公式

$$f(x)=\sum_{i=0}^{n}\frac{f(\alpha_i)(x-\alpha_0)(x-\alpha_1)\cdots(x-\alpha_{i-1})(x-\alpha_{i+1})\cdots(x-\alpha_n)}{(\alpha_i-\alpha_0)(\alpha_i-\alpha_1)\cdots(\alpha_i-\alpha_{i-1})(\alpha_i-\alpha_{i+1})\cdots(\alpha_i-\alpha_n)}$$

▷ ニュートン の補間公式

ニュートンの補間公式

$$f(x)=\lambda_0+\lambda_1(x-\alpha_0)+\cdots+\lambda_n(x-\alpha_0)(x-\alpha_1)\cdots(x-\alpha_{n-1})$$

（この式の $\lambda_0,\lambda_1,\cdots,\lambda_n$ は 次々に $x=\alpha_0,\cdots,\alpha_n$ を代入することによって得られる）

$f(\alpha_0)=\lambda_0$ として

$$f(\alpha_0,\cdots,\alpha_k,x)=\frac{f(\alpha_0,\cdots,\alpha_{k-1},x)-f(\alpha_0,\cdots,\alpha_k)}{x-\alpha_k}\qquad(1)$$

第4章 第22節

と定義すれば

$$\lambda_0 = f(\alpha_0),\quad \lambda_1 = f(\alpha_0,\alpha_1),\quad \cdots\cdots,\quad \lambda_m = f(\alpha_0,\cdots,\alpha_m)$$

傾き
差分商
差分係数

この $f(\alpha_0,\cdots,\alpha_k)$ のことを点 $\alpha_0,\cdots,\alpha_k$ に対する函数 $f(x)$ の k 次の傾き又は k 階の差分商［差分係数］という。

- k 階の差分商はまた，点 $\alpha_0,\cdots,\alpha_k$ で値 $f(\alpha_0),\cdots,f(\alpha_k)$ をとる 次数 k 以下の多項式の x^k の係数と定義してもよい。
- これから k 階の差分商は $\alpha_0,\cdots,\alpha_k$ の番号のつけ方に関係しない。

よって (1) 式の α_0 と α_k を入れかえて $x=\alpha_{k+1}$ とすると

$$\lambda_{k+1} = f(\alpha_0,\cdots,\alpha_{k+1}) = \frac{f(\alpha_1,\cdots,\alpha_{k+1}) - f(\alpha_0,\cdots,\alpha_k)}{\alpha_{k+1}-\alpha_0}$$

これから下記の差分商の表がつくられる。

$f(\alpha_0)$			
$f(\alpha_1)$	$f(\alpha_0,\alpha_1)$		
$f(\alpha_2)$	$f(\alpha_1,\alpha_2)$	$f(\alpha_0,\alpha_1,\alpha_2)$	
$f(\alpha_3)$	$f(\alpha_2,\alpha_3)$	$f(\alpha_1,\alpha_2,\alpha_3)$	$f(\alpha_0,\alpha_1,\alpha_2,\alpha_3)$
⋮	⋮	⋮	⋮

（これは左に並ぶ上下に隣り合う2つの値の差をとり $\alpha_k-\alpha_0$ で割ることにより得られる；なお n 次式の n+1 階の差分は 0 に等しくなる）

▷ 高次の算術数列

基礎の体は有理数体を含むとする。そして点 $\alpha_0,\alpha_1,\cdots,\alpha_m$ は相続く整数 $0,1,\cdots,n$ に等しくとる。$\alpha_k-\alpha_0=k$ だから $f(i)=a_i$ $(i=0,\cdots,n)$ に対してニュートンの公式を適応させために（$\deg f(x)\leq n$）
値の差を Δa_0 等で表わす。下記の表が得られる。

a_0				
a_1	Δa_0			
a_2	Δa_1	$\Delta^2 a_0$	$\Delta^3 a_0$	
a_3	Δa_2	$\Delta^2 a_1$	$\Delta^3 a_1$	$\Delta^4 a_0$
a_4	Δa_3	$\Delta^2 a_2$	⋮	⋮
⋮	⋮	⋮		

すると $\lambda_k = \dfrac{\Delta^k a_0}{k!}$ とる。$a_0,a_1,\cdots$ が n 次の多項式の値で

差分

あれば n+1 階の差分は0とる。列 $a_0,a_1,\cdots$ の n+1 階の差分が0に等しい時 $a_0,a_1,\cdots$ はニュートンの公式（$\lambda_k=\frac{\Delta^k a_0}{k!}$）によって与えられる多項式 $f(x)$（次数 $\leq n$）の値である。まず $\Delta^k a_0$ は明らかに等しい。$\Delta^{n+1} a_0=0$ だから $\Delta^n a_i$ の各値も一致する。次に $\Delta^{n-2} a_i$

みれば $\Delta^{m-1} a_i$ がすべて一致することからこれも等しいことがわかる。これを続ければ両方の $f(i)$ と a_i が一致することがわかる。

▷ 算術数列

差分の列が $n-1$ 次の算術数列であるような数列を n 次の算術数列という。但し同じ数だけから成る数列 $c\ c\ c\ \cdots$ を0次の算術数列という。

○ 点 $0, 1, 2, \cdots$ における n 次多項式 $f(x)$ の値は n 次の算術数列をなし逆に点 $0, 1, 2, \cdots$ における n 次の算術数列は高々 n 次の多項式の点 $0, 1, 2, \cdots$ の値からできている。n 次の算術数列の一般項 a_x は公式

$$a_x = f(x) = a_0 + x\Delta a_0 + \frac{x(x-1)}{2!}\Delta^2 a_0 + \cdots + \frac{x(x-1)\cdots(x-n+1)}{n!}\Delta^n a_0$$

によって値えられる。

注) 点が $0, 1, 2, \cdots$ でなく $0, h, 2h, \cdots$ の時は

$$\lambda_k = \frac{\Delta^k a_0}{k!\, h^k}$$ と置いて同様の公式がつくれる。但しその時は $x-1$ の代わりに $x-h$, $x-2$ の代わりに $x-2h$ をいれる。

Sm. 1 ○ n 次の算術数列の部分和 $S_m = \sum_{\nu=0}^{m-1} a_\nu$ ($S_0 = 0$) は

$$S_m = m a_0 + \binom{m}{2}\Delta a_0 + \cdots + \binom{m}{n+1}\Delta^n a_0$$

で求められる。

[証明] $S_{m+1} - S_m = \Delta S_m = a_m$ 故に $\Delta^k S_0 = \Delta^{k-1} a_0$ となる。故に $S_0 = 0$ から (S_x は $n+1$ 次の多項式だから)

$$S_m = 0 + m a_0 + \binom{m}{2}\Delta a_0 + \cdots + \binom{m}{n+1}\Delta^n a_0$$

Sm. 2 ○ 和 $\sum_{\nu=0}^{m-1} \nu$, $\sum_{\nu=0}^{m-1} \nu^2$, $\sum_{\nu=0}^{m-1} \nu^3$ の公式を求める。

[解答] $S_m = \sum_{\nu=0}^{m-1} \nu$ とすると $S_m = m a_0 + \binom{m}{2}\Delta a_0$ となる。$a_0 = 0$ $\Delta a_0 = 1$ から $S_m = \frac{1}{2} m(m-1)$

同様にして ν^2 について $S_m = \binom{m}{2}\Delta a_0 + \binom{m}{3}\Delta^2 a_0$, $\Delta a_0 = 1$, $\Delta^2 a_0 = 2$ だから $S_m = \frac{1}{6} m(m-1)(2m-1)$

ν^3 については $\Delta a_0 = 1$ $\Delta^2 a_0 = 6$ $\Delta^3 a_0 = 6$ だから

$$S_m = \binom{m}{2} + \binom{m}{3}\cdot 6 + \binom{m}{4} 6 = \frac{m^2(m-1)^2}{4}$$

索　引

< 諸 記 号 >

$a \in M$ … aはMの要素　(H, K) … Hの要素とKの要素の和の集合　$f'(x)$ … $f(x)$の導函数
$N \subseteq M$ … NはMの部分集合　G/N … NのGに対する剰余集合　Δa_0 … a_0における差分
$N \subset M$ … NはMの真部分集合　$M \cong N$ … MとNは同型である。　$\bar{a}$ … aの像
$A \cup B$ … AとBの合併集合　$a \equiv b \pmod{m}$ … mを法としてa, bは合同　$N(H)$ … 集合Hの正規化群
$A \cap B$ … AとBの共通集合　$R[x]$ … R上の多項式環(1元)
$M \sim N$ … MはNに準同型　(a) …… aによって生成される単項イデアル
$\{a\}$ … 生成元aの巡回群　(a, b) … a, bの最大公約元
HK …… Hの要素とKの要素の積集合　$N(\alpha)$ … αのノルム　例 $N(a+bi) = a^2+b^2$

1966・10・1 ～ 1966・12・29

本ノートは 洛北図書館
412 W1「現代代数学1」による