カントール

2次元平面は1次元の直線より多くの点を含む？

→ それぞれの点の集合は同じ濃度をもつことが証明された

→ 次元数は1対1対応によっていくらでも変わってしまう

→ 次元数を保存するために1対1対応に連続性の条件が必要

カントールの集合論の思考法

① 徹底した分析 → 無限集合の困難がでてくる

② すべてのものを空間化もしくは外延化する

↔内包，概念を広げること

集合算

$\in$ は $<, >$ と似ている

$\cap$ は乗算と似ている

$\cup$ は加算と似ている

$\overline{A}$ (補集合) は $-a$ と似ている

A：それ以外が成立する．Pを内包と呼べば部分集合Aは外延に当たる． ← 集合と論理のつながり

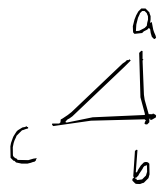
ブルバキは数学の様々構造を3種類に分類した

① 位相的構造

② 順序の構造

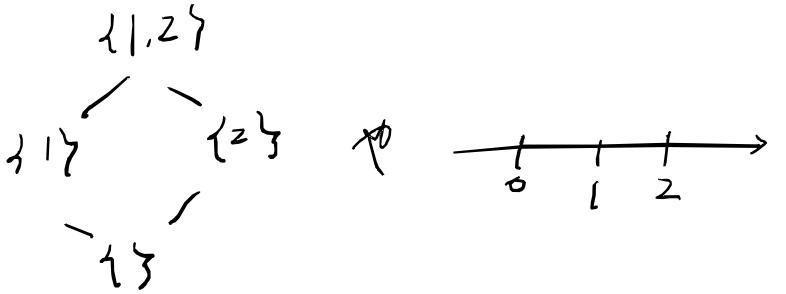
③ 代数的構造

位相的構造 … ある集合の要素間に近い/近い関係を考え出すこと



1. $a=b \to d(a,b)=0$, $a \neq b \to d(a,b)>0$
2. $d(a,b)=d(b,a)$
3. $d(a,c) \leqq d(a,b)+d(b,c)$

順序の構造



代数的構造

集合Eがあって、要素a,bから

$c=\varphi(a,b)$ をつくり出せる、φ という

関数が定義されているとき

Eを代数的構造という

$N=\{1,2,3\cdots\}$ は加法や乗法を考えると代数的構造

有限群の部分群の位数は、元の位数の約数となる

証明 $g \leqq G$, $g=\{a_1, a_2, \cdots, a_m\}$ とで

$bg=\{ba_1, ba_2, \cdots, ba_m\}$ をつくることを考え、

bg と cg が共通部分をもつとすると、$x \in bg$, $x \in cg$ がでる

$x=ba_i$, $x=ca_k$ とおこて

$$ba_i=ca_k, \quad b=(ca_k)a_i^{-1}=c(a_k a_i^{-1})$$

ここで bg の任意の要素を ba_l とすると、

$$ba_l=c(a_k a_i^{-1})a_l=c(a_k a_i^{-1}a_l)$$

つまり cg の要素ということになり、$bg \subseteq cg$ だし逆に $cg \subseteq bg$

$\rightarrow bg=cg$

bg, cg が共通部分をもつなら完全に同じ集合である

なので G のなかで重ならないように bg, cg, … をとっていく

bg, cg, … の類の個数を考えると、どれも等しくなる

$x=bg$ に左から cb^{-1} をかけると

$$cb^{-1}(bg)=cg$$ となり

$x'=cg$ も同様に $bc^{-1}(cg)=bg$ となる

類の数を l とすると、$|G|=l \times |B|$ (剰余群の位数)

$\rightarrow |G| \div |B|=l$

bg, hc などを右剰余類といい、gh, gc などを左剰余類という

剰余類は互いに交わらないし、大きさが同じなので

ある群 G の部分群の位数は G の位数の約数になる

定理 G の部分群 $g=\{a_1, a_2, \cdots a_r\}$ とし、G を g によって左剰余類に分けると、$gb_1, gb_2, \cdots, gb_s$ とする

このとき G の任意の要素は $a_i b_k$ $(i=1,2,\cdots r,\ k=1,2,\cdots,s)$ のただ一通りに書ける

証明 G は $gb_1, gb_2, \cdots, gb_s$ の和で書けるので、その要素は $a_i b_k$ の形で書ける

つぎに $a_i b_k = a_j b_l$ が等しいとすると、

$$b_k = a_i^{-1}(a_j b_l) = (a_i^{-1}a_j)b_l$$

$a_i^{-1}a_j$ は g に属するので b_k は gb_l の類に属する。したがって

$$b_k = b_l \Leftrightarrow k=l$$

(したがって $a_i = a_j(b_l b_k^{-1}) = a_j$

$\Leftrightarrow i=j$, つまり $a_i b_k$ は一通りに定まる

また、G は g と $B=\{b_1, b_2, \cdots, b_s\}$ の直積の形で

$G=g \times B$ とも書けることがわかる

正n形角を元の頂の上に重ねる操作の集合を D_n とおくと

D_n は群をつくる

このなかで折り返しを含まないものを $a = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 2 & 3 & 4 & \cdots & 1 \end{pmatrix}$ とすると

$a^n = e$ で $e, a, a^2, \cdots, a^{n-1}$ となる

たとえば正四角形だと、$a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ で

$a^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$, $a^4 = a^2 \times a^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = e$

折り返して b とすると $b = \begin{pmatrix} 1 & 2 & \cdots & n \\ n & n-1 & \cdots & 1 \end{pmatrix}$

$bab^{-1} = \begin{pmatrix} 1 & 2 & \cdots & n \\ n & n-1 & \cdots & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & \cdots & n \\ 2 & 3 & \cdots & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & \cdots & n \\ n & n-1 & \cdots & 1 \end{pmatrix}$

$= \begin{pmatrix} 1 & 2 & \cdots & n \\ n & 1 & \cdots & n-1 \end{pmatrix} = a^{-1}$ となる

作用の順番 → 右から

1は $1 \xrightarrow{b^{-1}} n \xrightarrow{a} 1 \xrightarrow{b} n$ になる。

2は $2 \xrightarrow{b^{-1}} n-1 \xrightarrow{a} n-1 \xrightarrow{b} 2$ になる。

両辺を m 乗すると

$(bab^{-1})^m = (a^{-1})^m$

$\longleftrightarrow (bab^{-1})(bab^{-1})\cdots(bab^{-1}) = (a^{-1})^m$ （m個）

ここで $(bab^{-1})(bab^{-1})$ をすると、$ba(b^{-1}b)ab^{-1}$

$= ba^2b^{-1}$ $(b^{-1}b = e$ だから$)$

$(bab^{-1})(bab^{-1})(bab^{-1})$ をすると $(ba^2b^{-1})(bab^{-1})$

$= ba^3b^{-1}$

よって $(bab^{-1})^m = ba^mb^{-1}$

だから $ba^mb^{-1} = a^{-m}$

D_n は $D_n = \{e, a, a^2, \cdots, a^{n-1}, b, ab, a^2b, \cdots, a^{n-1}b\}$

となる

ここには、$C_n = \{e, a, a^2, \cdots, a^{n-1}\}$ という部分群が含まれる

↑ 単一を要素とする巡回群

D_n は n 回分の回転 a という操作と

n 回分の反転 b という操作で表現できることを意味している

構造SとS'が同型である（$S \cong S'$）とは

1. Sの要素とS'の要素に1対1対応をつける
2. その対応によって関係がそのまま持ち越される

クラインの四元群　$G=\{00, 01, 10, 11\}$

	00	01	10	11
00	00	01	10	11
01	01	00	11	10
10	10	11	00	01
11	11	10	01	00

実数全体は加法について群であり、これをGとする

正の実数は乗法について群であり、これをG'とする

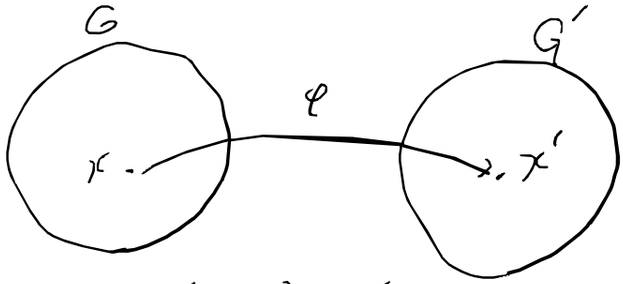
$x \in G$に対して、$x' \in G'$かつ$x'=a^x$ $(a>0, a\neq 1)$をとると

GとG'は同型

$$a^{\underbrace{x_1+x_2}_{G\text{の加法}}} = \underbrace{a^{x_1}\cdot a^{x_2}}_{G'\text{の乗法}} = x_1' \cdot x_2'$$

$G \to G'$を考えるのは指数関数で、

$G' \to G$を考えるのは対数関数



$$\varphi(x_1 x_2) = \varphi(x_1)\varphi(x_2)$$

$$\varphi(x^{-1}) = \varphi(x)^{-1}$$

が成立するときφはGからG'への同型写像

（同型対応）

$G \cong G'$

$\cong$の関係は　反射的　$G \cong G$

対称的　$G \cong G'$, $G' \cong G$

推移的　$G \cong G'$かつ$G' \cong G''$

$\to G \cong G''$

定理　1つの群Gの自己同型の全体は群をつくる

$A(G)$これをGの自己同型群という

部分集合の乗法

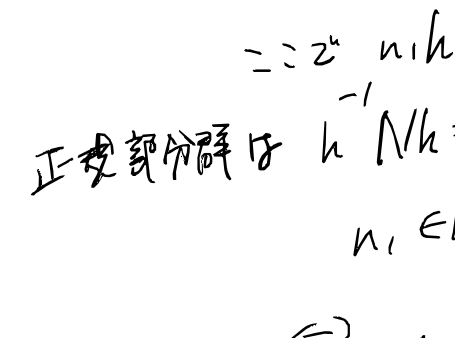
定理　Gの部分集合Aについて　$AA^{-1}\subseteq A$が成り立つなら
Aは部分群である

証明）集合Aが部分群であるために、以下を満たす必要がある
1、単位元eを含む
2、任意の元aの逆元を含む
3、任意の2つの元aの積を含む

1、$a\in A$をとると、$a^{-1}\in A^{-1}$, よって$aa^{-1}=e\in AA^{-1}$
仮定から$AA^{-1}\subseteq A$なので　$e\in A$

2、$a\in A$に対して$a^{-1}=ea^{-1}$になり、
$e\in A$, かつ$a^{-1}\in A^{-1}$だから$ea^{-1}\in AA^{-1}\subseteq A$
よって$a^{-1}\in A$

3、$a,b\in A$をとると、$b^{-1}\in A$はどこからわかるのか
$(b^{-1})^{-1}=b\in A^{-1}$よって$ab=a(b^{-1})^{-1}\in AA^{-1}\subseteq A$
なのでAの任意の2要素の積はAに含まれる



$\varphi(a)=a'$
$\varphi(b)=b'$とする

$\varphi(ab)=a'b'=\varphi(a)\varphi(b)$

G'はGに準同型
φはGからG'への準同型写像
とくにφが1対1対応のとき
同型となる

$gNg^{-1}\subset N$が成立する部分群$N\subset G$を正規部分群という
また任意の$g\in G, n\in N$に対して$gng^{-1}\in N$という

GをNによって剰余類に分けるとき
右剰余類と左剰余類は一致する
$gNg^{-1}=N$と考えてもよい

剰余類から商集合の候補を考えると
部分群$N\subseteq G$があるとき左剰余類$gN=\{gn\mid n\in N\}$
でGを分割できる
よって集合としての候補は$G/N:=\{gN\mid g\in G\}$

ここで剰余類同士の積を定義したい　$(gN)\cdot(hN):=(gh)N$
一方で代表元ghはどんな値をとっても結果が同じ剰余類になってほしい

つまり$gN=g'N$, $hN=h'N$なら$(gh)N=(g'h')N$

$gN=g'N$は$g'=gn_1$と同値とみなせて、同様に$h'=hn_2$

$g'h'=(gn_1)(hn_2)=g(n_1h)n_2$

ここでn_1hを$n_1h=h\cdot(n\text{の元})$とできれば都合がいい

正規部分群は$h^{-1}Nh=N\ (\forall h\in G)$で
$n_1\in N\Rightarrow h^{-1}n_1h\in N$

$\Leftrightarrow$　$n_1h=h(h^{-1}n_1h)$

これはNの元なので
$n_1h=hn_3\ (n_3\in N)$と書ける

$\therefore$　$g'h'=g(n_1h)n_2=g(hn_3)n_2=gh(n_3n_2)$

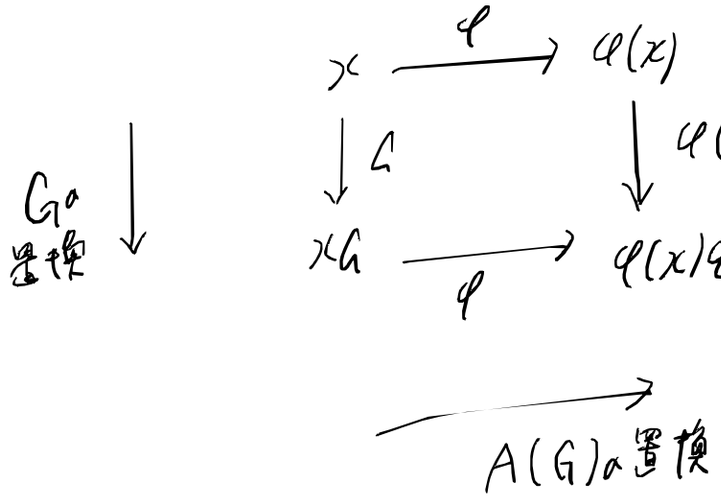
$n_3n_2\in N$なので　$g'h'\in ghN\Rightarrow(g'h')N=(gh)N$
ここで$(gN)(hN)=(gh)N$
はOK

有限群 $G=\{g_1, g_2, \cdots, g_n\}$ の自己同型の全体 $A(G)=\{\varphi_1, \varphi_2, \cdots\}$

対称群 S_n があるとき $A(G) \leqq S_n$

$a \in G$ は任意の要素 x に対して $x \to xa$ という置換を引き起こす

さらに $\varphi(xa)=\varphi(x)\varphi(a)$



$\varphi^{-1}a\varphi$ をつくると、これは G に属する

逆に、$g_i, g_k \in G$ とすると $\varphi^{-1}g_i g_k \varphi = \varphi^{-1}g_i\varphi \cdot \varphi^{-1}g_k\varphi$

からこのような φ は自己同型を引き起こす

※1 自己同型とは群を壊さない対称性、対称群の中での共役操作として記述できる

$A(G) \supseteq B \supset C$ が成り立つとは、群の構造的対称性は置換としての対称性に持ち上げられること

- $A(G)$：自己同型群
- B：正規化群 — 動かす自由度
- C：安定化群 — 動かしても変わらない部分

$a, b \in G$ が $x \in G$ のとき 以下の関係があるとき a, b は互いに共役である

$b = xax^{-1}$

共役は同値律を満たす

反射的：$a = eae^{-1} = a$ （$x=e$ とする）

対称的：$b = xax^{-1}$ ならば $a = x^{-1}bx = (x^{-1})b(x^{-1})^{-1}$

推移的：$xax^{-1}=b$, $x'bx'^{-1}=c$ ならば

$c = x'(xax^{-1})x'^{-1} = (x'x)a(x'x)^{-1}$

よって $a \sim b$ と表すことができる

共役で G をいくつかの類に分類するとき各々の類を共役類という

定理　有限群Gの共役類の個数はGの位数の約数である

証明）　共役類Cの要素をaとする。Cは xax^{-1} 全体の集合 $(x \in G)$

Gのなかで $xax^{-1}=a$ となる要素全体の集合を $k(a)$ とする

$eae^{-1}=a$ だから $e \in k(a)$

また、$x \in k(a)$ ならば $xax^{-1}=a$.

左から x^{-1}, 右から x をかけると $a=x^{-1}ax=x^{-1}a(x^{-1})^{-1}$ から

$$x^{-1} \in k(a)$$

また、$x, x' \in k(a)$ なら $xax^{-1}=a$ に

左から x', 右から x'^{-1} をかけると $x'xax^{-1}x'^{-1}=x'ax'^{-1}$

$$\longleftrightarrow (x'x)a(x'x)^{-1}=a$$

$$x'x \in k(a)$$

よって $k(a)$ は部分群

ここで $C=\{a_1, a_2, \cdots a_r\}$ とすると $(a_1=a)$

$xa_1x^{-1}=a_k$

$x'a_1x'^{-1}=a_k$ ↘ となる x があり、

から ↪ $x^{-1}x'a_1x'^{-1}x = x^{-1}a_kx = a_1$ だから

$$x^{-1}x' \in k(a_1)$$

$$x' \in xk(a_1)$$ 右剰余類の形

途中で $x' \in xk(a_1)$ ならば $k(a_1)$ に属する x'' をとれば

$x'=xx''$ とすることができる

$x'a_1x'^{-1}=xx''a_1x''^{-1}x^{-1}=xa_1x^{-1}=a_k$

つまり $xa_1x^{-1}=a_k$ となるGの要素は $k(a_1)$ の剰余類

したがって $a_1, a_2, \cdots a_r$ は $k(a_1)$ の剰余類と

1対1対応

Gの位数を n, $k(a_1)$ の位数を m とすれば

$r=\frac{n}{m}$, r は n の約数

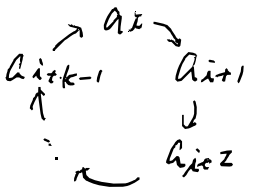
ラグランジュの定理より

対称群の共役類

n次対称群 S_n の位数は $n!$、この群の共役類を求める

置換Sは巡回する環に分かれる

$(a_i, a_{i+1}, \cdots, a_{i+k-1})$



いくつかの環に分かれるので $(a_1, a_2, \cdots, a_l)(a_{l+1}, \cdots, a_{l+m})\cdots(\ )\cdots$

$n = l + m + \cdots$

この巡環の長さが1つずつ一致する他の置換

$S' = (a_1', a_2', \cdots, a_l')(a_{l+1}', \cdots, a_{l+m}')\cdots$ があり、

ここで $X = \begin{pmatrix} a_1' & a_2' & \cdots & a_l' & a_{l+1}' & \cdots \\ a_1 & a_2 & \cdots & a_l & a_{l+1} & \cdots \end{pmatrix}$ を考えると

$X^{-1} = \begin{pmatrix} a_1 & a_2 & \cdots & a_l & a_{l+1} & \cdots \\ a_1' & a_2' & \cdots & a_l' & a_{l+1}' & \cdots \end{pmatrix}$ となり

XSX^{-1} という置換は、 $a_i' \xrightarrow{X} a_i \xrightarrow{S} a_{i+1} \xrightarrow{X^{-1}} a_{i+1}'$ なので

$a_i' \to a_{i+1}'$ となり、これは S' に等しい

したがって $XSX^{-1} = S'$

逆にこのような S, S' 環の長さは等しい、$l, m, \cdots$ という長さは1つの共役類と対応する

S_1 を考えると $1=1$ しかないから共役類は1

S_2 は $2=2=1+1$ だから共役類は2

S_3 は $3=3=2+1=1+1+1$ だから共役類は3

S_4 は $4=4=3+1=2+2=2+1+1=1+1+1+1$

だから共役類は5

群Gのなかで他のすべての要素と交換可能な

要素の集合をGの中心という

定理　中心はGの正規部分群をつくる

定理　1つの素数pの累乗 p^r を位数にもつ群は単位群より大きい中心をもつ

証明）群Gの位数が p^r とする、共役類の個数Gの位数 p^r の約数であることがわかっていて、一方で単位元eからできる共役類の個数は1である

もしその他の共役類の個数がすべてpの倍数であったら

$p^r = 1 + p(\cdots)$

が成り立つことになり、矛盾する

したがって共役類 $[e]$ 以外にも個数1の共役類が存在する

このようなGはGのすべての要素と交換可能なので

中心に属する、だから中心は単位元以外の要素をもつ、

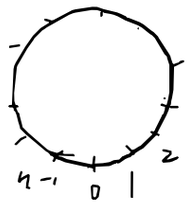
複合構造 ⟶ 分析 ⟵ 総合 単構造

上記のような考え方を有限可換群に適用してみる

$\mathbb{Z} = \{\cdots, -3, -2, -1, 0, 1, 2, 3, \cdots\}$

は+1と逆元-1からすべての要素がつくられる単生群である

このような有限の単生群を考えると、 $\underbrace{1+1+\cdots+1}_{n} = 0$



乗法で考えると、 $G = \{e, a, a^2, \cdots, a^{n-1}\}$ $(a^n = e)$ となり

このような有限の単生群を巡回群とよぶのであった

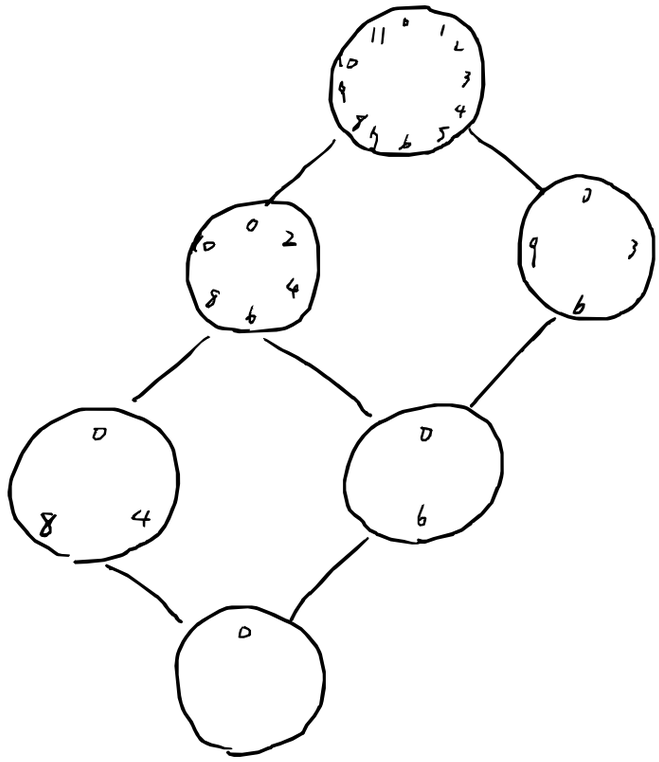
定理　位数 n の巡回群の部分群はすべてまた巡回群であり、

n の任意の約数 g に対しては、g を位数とする部分巡回群が1つだけ含まれる

定理　d' が d の倍数であるとき、a^d によって生成される部分群を

$S(d)$ とすると、$S(d')$ は $S(d)$ の部分群であり、逆も成り立つ

例)



位数12の巡回群とは、文字盤の数字は G^n の指数 n に対応する

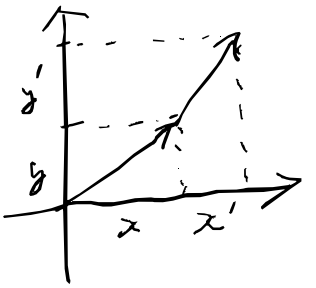
巡回群は12の約数の6だけの

部分群を有する

2次元ベクトル全体を加法について群 V_2 とする.

要素 $a=[x,y]$, $a'=[x',y']$ とすると

$a+a'=[x+x', y+y']$



1. V_2 の任意の要素は X と Y の要素の和で表される

$[x,0]$ $[0,y]$

2. X と Y の共通部分は V_2 の単位元だけである

$[0,0]$

このとき V_2 は X と Y の直和であり, 積の形では直積である

$V_2 = X+Y$

一般に $[a,b][a',b']=[aa',bb']$ となるとき $[a,b]$ は2つの群の直積

$A\times B$ で表す.

定理 可換とは限らない群 G の中に正規部分群 A, B が含まれ

1. G の要素が A, B の要素の積で表され

2. $A\cap B=\{e\}$

このとき $G=A\times B$

定理　可換群は素数の累乗を位数とする可換群の直積に分解する

位数が素数の累乗とは?

→ 群の元の個数が p^n 個, p は素数

2^3

3^2

5^1

⋮

$\mathbb{Z}/8\mathbb{Z} = \{0,1,2,3,4,5,6,7\}$

位数は $2^3=8$ の可換群

あるいは $\mathbb{Z}/6\mathbb{Z} = \{0,1,2,3,4,5\}$

位数6の可換群

$= 2 \times 3$

素数　素数

$\mathbb{Z}/2\mathbb{Z}$　$\mathbb{Z}/3\mathbb{Z}$ に分けられる

直積は $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$

なので $\mathbb{Z}/6\mathbb{Z} = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$

が成り立つ

元を書くと $\{0,1,2,3,4,5\}$

$= \{(0,0),(0,1),(0,2),(1,0),(1,1),(1,2)\}$

$\overrightarrow{\varphi(\bmod 2, \bmod 3)}$ の写像をとっている

$0 \bmod 2 = 0$, $0 \bmod 3 = 0$ → $(0,0)$

$1 \bmod 2 = 1$, $1 \bmod 3 = 1$ → $(1,1)$

$2 \bmod 2 = 0$, $2 \bmod 3 = 2$ → $(0,2)$

$3 \bmod 2 = 1$, $3 \bmod 3 = 0$ → $(1,0)$

$4 \bmod 2 = 0$, $4 \bmod 3 = 1$ → $(0,1)$

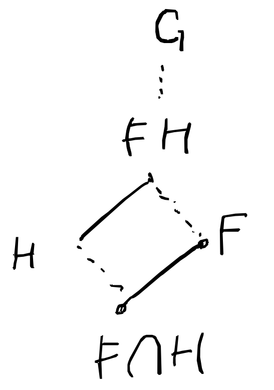
$5 \bmod 2 = 1$, $5 \bmod 3 = 2$ → $(1,2)$

素数の累乗 p^n を位数とする可換群Gを巡回群の直積にできるらしいが証明がむずかしい...

第1同型定理　群Gのなかに正規部分群Hと部分群Fがある

FHはGの部分群となり、$F\cap H$は

Fの正規部分群となる、このとき $FH/H \cong F/(F\cap H)$



証明）仮定からHは正規部分群なので

$(FH)(FH)^{-1} = (FH)(H^{-1}F^{-1}) = FHH^{-1}F^{-1} = FHF = FFH = FH$（可換）

↳ Hは部分群なので $H = H^{-1}$

よって $FHH^{-1}F^{-1} = FHHF^{-1}$

また、$HH = \{h_1h_2 \mid h_1, h_2 \in H\} = H$

よって FHF^{-1}となる

正規性 $\forall f \in F \subset G,\ fHf^{-1} = H$ から

$FHF^{-1} = H$

FHはGの部分群であることが定まる。

$x \in F\cap H$, $f \in F$とすると $fxf^{-1} \in H$でありかつ $fxf^{-1} \in F$

したがって $fxf^{-1} \in F\cap H$となり

$F\cap H$はFの正規部分群である

$F/(F\cap H)$の剰余類を $F\cap H$, $(F\cap H)a_1$, …, $(F\cap H)a_r$ とする

$a_1, a_2, \dots a_r \in F$

ここでFH/Hのなかで $H, Ha_1, Ha_2, \dots, Ha_r$という集合を考える

$f_1h_1 \in FH$とすると $f_1 \in (F\cap H)a_i$

したがって FHは $H, Ha_1, Ha_2, \dots Ha_r$の合併集合に等しい

$FH = [(F\cap H) \cup (F\cap H)a_1 \cup \dots]H$であり

$(F\cap H)H$

$(F\cap H)a_1H$

⋮

と分解でき、

$F\cap H$はHの要素でHは部分群なので

$(F\cap H)H$はHからはみ出さない

次に$(F\cap H)a_1H$でHはGの正規部分群なので$a_1H = Ha_1$であり、

$(F\cap H)a_1H = Ha_1$となる

$a_2, a_3, \dots a_r$も同様

よって $FH = H \cup Ha_1 \cup Ha_2 \dots \cup Ha_r$

→ Fの代表元としてaをとっても、そのままより大きなFHという群においても、Hを基準として剰余類の代表として使える

$H, Ha_1, \dots Ha_r$は互いに共通部分を有しない

もし有するなら　$h_ia_i = h_ka_k$　$(h_ia_i \in Ha_i,\ h_ka_k \in Ha_k)$

$a_ia_k^{-1} = h_i^{-1}h_k \in H$

一方 $a_ia_k^{-1} \in F$から $a_ia_k^{-1} \in F\cap H$

$(F\cap H)a_i$と$(F\cap H)a_k$が異なる剰余類である仮定に反する。

ここでFH/Hの剰余類と$F/(F\cap H)$の剰余類のあいだには

$Ha_i \rightleftarrows (F\cap H)a_i$

の1対1対応が存在する。右辺が左辺の部分集合

イメージ）メモ　より小さな世界であるFのなかでa_iというもので世界をわける構造はより大きなFHのなかでも維持される

また　$Ha_i \times Ha_k = H(a_ia_k)$

$(F\cap H)a_i \times (F\cap H)a_k = (F\cap H)(a_ia_k)$

で どちらも同じかけ算のルールをもつことにもなり

その対応は同型対応となっている

第1章 環と体

ペアノの公理から自然数の集合 $\mathbb{N}$ のなかに要素 a の1対1写像 $\varphi(a)$ が存在し $\varphi(a)=1$ となる a は存在しない

$\mathbb{N}$ から $\mathbb{Z}$ を構成する

$a, b \in \mathbb{N}$ の組 $[a,b]$ を考える。2次元ベクトルと考えてもよい

$[a,b]$ 全体の集合を $\mathbb{N}^2$ と表す

$[a,b], [c,d] \in \mathbb{N}^2$ は $a+d=b+c$ のとき $[a,b] \sim [c,d]$ と定義する

$[a,b] \sim [c,d]$ は同値律を満たす

反射律：$a+b=b+a$ だから $[a,b] \sim [a,b]$

対称律：$[a,b] \sim [c,d]$ ならば $a+d=b+c$

したがって $b+c=a+d$, $c+b=d+a$

$\therefore [c,d] \sim [a,b]$

推移律：$[a,b] \sim [c,d]$, $[c,d] \sim [e,f]$ なら

$a+d=b+c$ 両辺に f を加えて

$a+d+f=b+c+f$、$[c,d] \sim [e,f]$ だから

$c+f=d+e$ から

$=b+d+e$

したがって $(a+f)+d=(b+e)+d \Leftrightarrow a+f=b+e$

$\therefore [a,b] \sim [e,f]$

$[a,b]+[c,d]=[a+c, b+d]$ の加法を導入し、

$[a,b] \sim [a',b']$

$[c,d] \sim [c',d']$ のとき $[a,b]+[c,d] \sim [a',b']+[c',d']$

証明) $[a+c, b+d] \sim [a'+c', b'+d']$ を証明する

$[a,b] \sim [a',b']$ だから $a+b'=a'+b$

$[c,d] \sim [c',d']$ だから $c+d'=c'+d$

$(a+c)+(b'+d')=(b+d)+(a'+c')$

$=(a'+b)+(c'+d)$

$=(a'+c')+(b+d)$

だから $[a+c, b+d] \sim [a'+d, b'+d']$

$[a,b]+[c,d] \sim [a',b']+[c',d']$

$[c,c]$ は 0 と同じ役割として導入する

$[a,b]+[c,c]=[a+c, b+c]$

ここで $a+(b+c)=a+(c+b)=(a+c)+b$

$\therefore [a,b] \sim [a+c, b+c]$

$[c,c]$ と加えても類の中を変えるだけで類は変わらない

$[a,b]+[b,a]=[a+b, b+a]=\underline{[a+b, a+b]}$

$[c,c]$ の形なので0

よって $[b,a]=-[a,b]$ としてもよい

大小について $b+c < a+d$ のとき $[a,b] < [c,d]$ とする

大小関係の推移律を証明する

$[a,b] < [c,d]$, $[c,d] < [e,f]$ のとき $[a,b] < [e,f]$

$(b+e)+c = b+c+e = (b+c)+e < (a+d)+e$

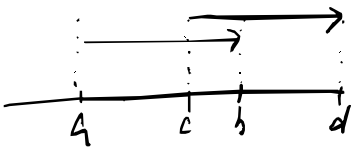
$= a+(d+e) < a+(c+f)$

$= (a+f)+c$

(だから $b+e < a+f$

$\therefore [a,b] < [e,f]$ 」

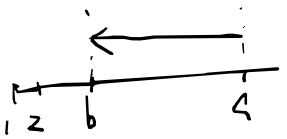
これを $\mathbb{Z}'$ と表すと、$\mathbb{Z}'$ は大小の順序をもつ



$[a,b]$ をベクトルと考えると、

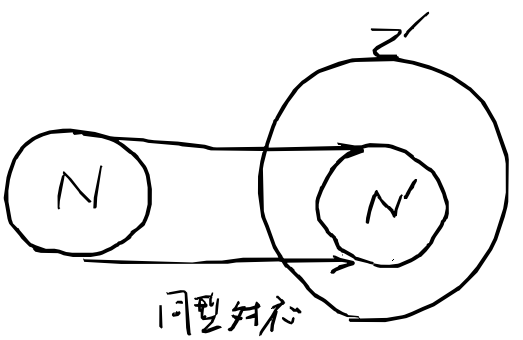
$a+d = b+c$ となる $[c,d]$ に移動しても

ベクトルとしては同一とみなせる



$a=b$ なら 0,

$a>b$ ならマイナスと考えられる



$\mathbb{Z}'$ は $+,-,\times$ をもつ整数の集合と同型

N を拡大して $\mathbb{Z}$ をつくったと考えてもよい

$\mathbb{Z}$ に乗法を定義する、$[a,b]\cdot[c,d]$ を考える

$a<b$, $c<d$ のとき $b-a$, $d-c$ に対応する

$$(b-a)(d-c)=bd+ac-ad-bc$$
$$=(bd+ac)-(ad+bc)$$

$[a,b][c,d]=[ad+bc,\ bd+ac]$ と定義するとよさそうである

$[a,b][c,d]\sim[a',b'][c',d']$ を証明する

$[a,b][c,d]=[ad+bc,\ ac+bd]$

$[a,b][c',d']=[ad'+bc',\ ac'+bd']$

ここで $(ad+bc)+(ac'+bd')=ad+bc+ac'+bd'$

$$=a(d+c')+b(c+d')$$

$[c,d]\sim[c',d']$ だから

$c+d'=d+c'$

$$=a(c+d')+b(c'+d)$$
$$=ac+bd+ad'+bc'$$

よって $[a,b][c,d]\sim[a,b][c',d']$

また $[a,b][c',d']\sim[a',b'][c',d']$

$\therefore\ [a,b][c,d]\sim[a',b'][c',d']$

このあとの証明、左分配則の証明、結合法則の証明など煩雑となり方針として

スマートではない

この定義は $\mathbb{N}$ にこだわりたとえば無理数などの存在を認めない立場をとる

環の性質

+, ×をもつ集合R

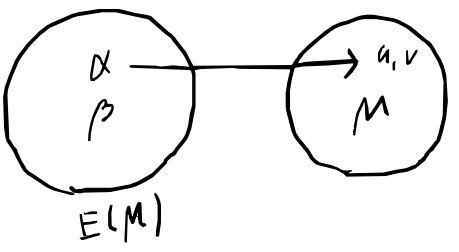
1. 加法について可換群をなす, $a+b=b+a$
   単位元は0 $a+0=a$
   逆元は$-a$ $a+(-a)=0$
2. 乗法について結合法則がなりたつ $(ab)c=a(bc)$
3. 加法、乗法に分配法則がなりたつ $a(b+c)=ab+ac$
   $(b+c)a=ba+ca$

乗法の交換法則 $ab=ba$ が成り立つとき可換環

(例) Rを任意の環としたとき、Rの要素を係数とする
多項式 $a_0x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n$
は多項式の加法と乗法について環をつくる。
不定元xをもつ多項式環といい、$R[x]$で表わす

(例) 環Rの要素を行列の要素とする n次正方行列
$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}$ は行列の加法・乗法について環をつくる
行列環

(例)



加群M(可換)をMに同型に写す写像α
$u\in M \xrightarrow{\alpha} \alpha u$
$\alpha(u+v)=\alpha u+\alpha v$
を満たす準同型全体をE(M)

E(M)は以下の+, ×の定義で環をつくる

+) $(\alpha+\beta)u=\alpha u+\beta u$ とすると
$(\alpha+\beta)(u+v)=\alpha(u+v)+\beta(u+v)$
$=\alpha u+\alpha v+\beta u+\beta v$
$=(\alpha+\beta)u+(\alpha+\beta)v$

よって $\alpha+\beta\in E(M)$

×) $\alpha\beta(u)=\alpha(\beta(u))$ とすると
$\alpha\beta(u+v)=\alpha(\beta(u+v))$
$=\alpha(\beta u+\beta v)$
$=\alpha(\beta(u))+\alpha(\beta(v))$
$=\alpha\beta(u)+\alpha\beta(v)$

よって $\alpha\beta\in E(M)$

すべてのuを0に写す ϕ もE(M)に含まれ
$\phi(u+v)=0$, $\phi(u)=0$, $\phi(v)=0$ から
$\phi(u+v)=\phi(u)+\phi(v)$ なので $\phi\in E(M)$

また $\alpha+\phi=\alpha$
つぎに、$(-\alpha)(u)=-\alpha(u)$ となる$-\alpha$を考えると
$\alpha+(-\alpha)=0$ は明らか
また $(\alpha+\beta)(u)=\alpha(u)+\beta(u)=\beta(u)+\alpha(u)=(\beta+\alpha)(u)$
から $\alpha+\beta=\beta+\alpha$
ほしく $(\alpha+\beta)+\gamma=\alpha+(\beta+\gamma)$
よって E(M)は加法について加群をなす

乗法について $(\alpha\beta)\gamma(u)=\alpha(\beta(\gamma(u)))$
$\alpha(\beta\gamma(u))=\alpha(\beta(\gamma(u)))$ から
$(\alpha\beta)\gamma=\alpha(\beta\gamma)$
よって 結合法則を満たす

また. $\alpha(\beta+\gamma)(u)=\alpha(\beta(u)+\gamma(u))$
$=\alpha(\beta(u))+\alpha(\gamma(u))$
$=\alpha\beta(u)+\alpha\gamma(u)$
$=(\alpha\beta+\alpha\gamma)(u)$

よって $\alpha(\beta+\gamma)=\alpha\beta+\alpha\gamma$
同様に $(\beta+\gamma)\alpha=\beta\alpha+\gamma\alpha$

→ E(M)は環をつくることが証明できた
E(M)をMの自己準同型環という

2つの環が同型 $R \cong \bar{R}$, 任意の要素 a, b に対して

$\varphi(a \pm b) = \varphi(a) \pm \varphi(b)$

$\varphi(ab) = \varphi(a)\varphi(b)$ となる φ が存在すること

$\varphi(R) = \bar{R}$ で φ が全射のとき $\bar{R}$ は R に準同型

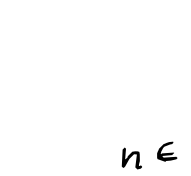
R のイデアル I : $R \to \bar{R}$ の 0 になる φ をもつ R の部分集合

$I \subseteq R$ のとき、$a - b \in I$ となると $a \equiv b \pmod{I}$

=この関係が同値律をみたす

↓

R の I による剰余類



$a - b \in I$, $c - d \in I$ となる要素をとりだすと

$a \equiv b \pmod{I}$ $c \equiv d \pmod{I}$

$(a+c) - (b+d) = \underbrace{(a-b)}_{\in I} + \underbrace{(c-d)}_{\in I}$

$\longleftrightarrow$ $a + c \equiv b + d \pmod{I}$

また $ac - bd = ac - ad + ad - bd$

$= a\underbrace{(c-d)}_{\in I} + \underbrace{(a-b)}_{\in I} d$

$\longleftrightarrow$ $ac \equiv bd \pmod{I}$

よって 三はニと同じく辺ごとの加法乗法ができる

剰余類を1つの要素とみなしてうまれた環を剰余環といい、R/I で表す

$R \xrightarrow{\varphi} R/I$ と写す φ は準同型

群における正規部分群と

環におけるイデアルは類似の役割

$\mathbb{Z} = \{\cdots -1, 0, 1 \cdots\}$, のイデアルを I とする

$n \in I$ となる正の数のうち最小の数を考える

$x \in I$ をとり n で割ると

$x = qn + r \quad (0 \leq r < n)$

$r = x - qn$

$n \in I$ から $qn \in I$ よって $x - qn \in I$

$r > 0$ ならば $r < n$ だから r が I の要素になってしまうことに矛盾する。(n が I のなかで最小と仮定しているので)

∴ $r = 0$ したがって $x = qn$

x は n の倍数であり、I は n のすべての倍数の集合、

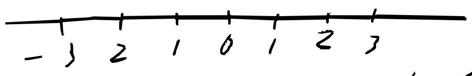
これを (n) とする.

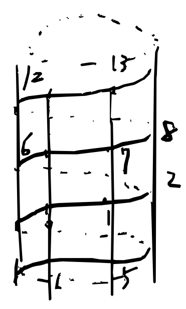
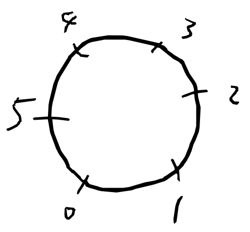
$I = (n)$ とすると $a \equiv b \pmod{I}$ は

$a \equiv b \pmod{n}$ とかけ

$a - b$ は n の倍数である

ガウスの合同式

ℤ/(1) という環を考える  という直線を

円柱に巻きつけて  と考えて上からみると 

体の定義　環のうち0以外の要素は乗法に対して群をつくるとき体という
乗法の単位元を e で表す

例) 1. 有理数全体
2. 実数全体
3. 複素数体
4. 4元数体（乗法は可換でない）　$a1+bi+cj+dk$

体では0ではない2つの元をかけて0となることはない
$a\neq0,\ b\neq0$ で $ab=0$ となる場合を考える
a^{-1}を両辺にかけて　$a^{-1}ab=a^{-1}0=0$
∴ $b=0$ となり $b\neq0$ に反する

可換体の分類　体Fの乗法の単位元 e を加え加えていく
$\underbrace{e+e+e+e+e+\cdots}_{n}=0$　となる場合を考える

nは素数でないとすると $n=lm$　このとき
$\underbrace{(e+e+\cdots+e)}_{l}\underbrace{(e+e+\cdots+e)}_{m}=\underbrace{(e^2+e^2+\cdots+e^2)}_{lm}$
↳ $\sum_{i=1}^{l}\sum_{j=1}^{m}e\cdot e$　　$e^2=e$ なので（単位元だから）
$=\underbrace{(e+e+\cdots+e)}_{n}=0$

$\frac{nnnnn}{15}$

$\underbrace{(e+e+e\cdots+e)}_{l}$ か $\underbrace{(e+e+e+e+\cdots+e)}_{m}$ のどちらかは
0にならないといけないので $n=lm$ は矛盾
eの数を素数 p で表す
↑ 体Fの標数という

次にFのなかの最小の体を考える
$0,\ e,\ e+e,\ \cdots,\ \underbrace{e+\cdots+e}_{p-1}$ を
$0,\ e,\ 2e,\ \cdots,\ (p-1)e$ で表すと p個の要素は
$P=\{0, e, 2e, \cdots, (p-1)e\}$　$[pe=0]$

Pは環をなす ⟵ $le\pm me=(l\pm m)e$
$(le)(me)=(lm)e^2=(lm)e$

ここで $a\in P$ であり $a\neq0$ となるaで考え、Pのなかで $x\to ax$ の写像
$ax=ay \Leftrightarrow a(x-y)=0 \Leftrightarrow x=y$ となるので　をとる
$a\neq0$だから
$x\to ax$は1対1写像、よって ax は e ともなる
$ax=e$ となる x は a の逆元である。
Pの0でない要素がすべて逆元をもつから Pは体である
↗ Fのなかで最小の体で
素体という
↗ ℤ/(p)と同型

$e+e+\cdots+e=0$ とならない場合
Fの標数は0
このとき素体は有理数体と同型

※ 実数体、複素数体は最小でないので素体とならないし、非可算無限でサイズが異なるので同型とならない

$F_2 = \{0, e\}$, $2e = 0$ とおくと

+	0	e
0	0	e
e	e	0

×	0	e
0	0	0
e	0	e

$1+1 \equiv 0 \pmod 2$
となるeなら他のものにしてもよい

記号論理学を考えると、命題A, B, C, ⋯があったとき

AandBは $A \wedge B$ で表すと

A	B	$A \wedge B$
0	0	0
1	0	0
0	1	0
1	1	1

なるべく $A \times B$ と同じ

A or B は $A \vee B$ で表すと

A	B	$A \vee B$
0	0	0
1	0	1
0	1	1
1	1	1

なるべく $A + B + A \times B$ と同じ

not A は $\bar{A}$ で表すと

A	$\bar{A}$
0	1
1	0

なるべく $1 - A$ と同じ

A, B, C, ⋯ を $\wedge \vee -$ で表すことは $+ \times -$ で多項式 $\varphi(A, B, C, \cdots)$ と同じ

$\underbrace{A, B, C, \cdots}_{n}$ とすると 2^n 通りあり、φ もまた0か1かどちらかを取るので このような φ の個数は $2^{(2^n)}$ である

$\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$ の行列でつくる環を考えると

$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ となる

これらを零因子と呼ぶ

乗法の単位元の1をもち、零因子を含まない可換な環を整域という

定理　整域Rに不定元X, Y, Z, ⋯を付加して得られる多項式環 $R[X, Y, Z, \cdots]$ はやはり整域

整域Rの要素 a, b を考え (a,b) と表わし、これは a/b だとする
$b \neq 0$ と仮定

(a,b) はRの要素を成分とする2次元ベクトルと考えてもよい
$ad = bc$ のとき 同値とみなして $(a,b) \sim (c,d)$ とかく

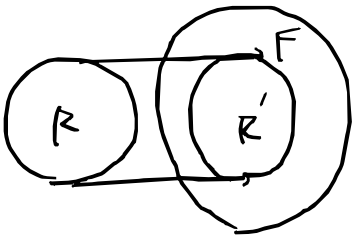
同値律を確認できる

$(a,b)+(c,d) = (ad+bc, bd)$ を加法とすると
交換法則
結合法則
0
逆元 が成り立つ

$(a,b)(c,d) = (ac, bd)$ を乗法とすると
交換法則
結合法則
分配法則
単位元
逆元 が成り立つ

∴ 体をなす

この体をFとするとRの商体という



Fの中にRと同型な環R'が含まれることを確認し、Rを体Fまで拡大したものと考えたい

$a \in R$, $(c,1) \in F$ とおく
$a \longrightarrow (a,1)$
$b \to (b,1)$ とし、$(a,1) \sim (b,1)$ のとき $a-1 = 1-b$
$\therefore a = b$

つまり $(a,1)$ には1つの a だけが対応する

つぎに、$(a,1) \pm (b,1) = (a-1 \pm 1-b, 1-1) = (a \pm b, 1)$ が言える

$$\begin{array}{ccccc} a & + & b & = & a+b \\ \uparrow & & \uparrow & & \uparrow \\ (a,1) & \pm & (b,1) & = & (a \pm b, 1) \end{array}$$

で加減は同型

$(a,1) \cdot (b,1) = (ab, 1 \cdot 1) = (ab, 1)$

$$\begin{array}{ccccc} a & \times & b & = & ab \\ \uparrow & & \uparrow & & \uparrow \\ (a,1) & \times & (b,1) & = & (ab, 1) \end{array}$$

で乗法も同型

∴ R'とRは同型

Rは1をもつ可換環とし、$R[x_1, x_2, \cdots, x_n]$のなかの要素$f(x_1, x_2, \cdots x_n)$が$x_1, x_2, \cdots x_n$のどのような入れ換えでも不変なとき

$f(x_1, x_2, \cdots x_n)$を$x_1, x_2, \cdots x_n$の対称関数
もしくは対称多項式という。

$R[x_1, x_2]$では x_1+x_2や$x_1^2+x_2^2$は対称関数
x_1-x_2や$x_1^2x_2$は〃 ではない

$(y-x_1)(y-x_2)\cdots(y-x_n)$という対称関数を展開したとき

$= y^n - (x_1+x_2+\cdots+x_n)y^{n-1}$
$+ (x_1x_2+\cdots+x_{n-1}x_n)y^{n-2}$
$- \cdots \pm x_1x_2\cdots x_n$

$\sigma_1 = x_1+x_2+\cdots+x_n$
$\sigma_2 = x_1x_2+x_2x_3+\cdots+x_{n-1}x_n$
$\vdots$
$\sigma_n = x_1x_2\cdots x_n$

とすると
$y^n - \sigma_1 y^{n-1} + \sigma_2 y^{n-2} - \cdots \pm \sigma_n$

σは基本対称関数

ex. $n=2$のとき
$(y-x_1)(y-x_2)$
$= y^2 - x_1y - x_2y + x_1x_2$
$= y^2 - (x_1+x_2)y + x_1x_2$

$n=3$のとき
$(y-x_1)(y-x_2)(y-x_3)$
$= (y^2-(x_1+x_2)y+x_1x_2)(y-x_3)$
$= y^3 - (x_1+x_2)y^2 + x_1x_2y$
$- (x_3y^2 - (x_1+x_2)x_3y + x_1x_2x_3)$
$= y^3 - (x_1+x_2+x_3)y^2$
$+ (x_1+x_2)(x_3+1)y$
$- x_1x_2x_3$

$x_1+x_2+x_1x_3+x_2x_3$

定理 Rにおけるn変数の対称関数は
Rの要素を係数とする$\sigma_1, \sigma_2, \cdots \sigma_n$の多項式で表される

有理数体 $\subset$ 実数体 $\subset$ 複素数体

一般に $F \subseteq F'$ のとき
FをF'の部分体
F'をFの拡大体という

体F ⊂ 体Ω
集合MとFを含む最小の体を$F(M)$とする
$\alpha \in M$がありMの要素がαだけのとき
$F(\alpha)$はFの単純拡大であるという

既約多項式を手がかりとして体の拡大を行う

例) 有理数体 $\mathbb{Q}$ のなかで $\varphi(x)=x^2-x-1$ を考えると $\mathbb{Q}$ のなかで既約

$\mathbb{Q}[x]/(x^2-x-1)$ の各要素は任意の多項式

$f(x)=q(x)(x^2-x-1)+(a+bx)$ から

$f(x)\equiv a+bx \pmod{(x^2-x-1)}$ である

和は $(a+bx)+(a'+b'x)=(a+a')+(b+b')x$

乗法は $(a+bx)(a'+b'x)=aa'+(ab'+a'b)x+bb'x^2$

x^2-x-1 で割る

$x^2-x-1=0$ なので $x^2=x+1$

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

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

$bb'x^2\equiv bb'(x+1)$

$=aa'+(ab'+a'b)x+(bb'x+bb')$

$=(aa'+bb')+(ab'+a'b+bb')x$

$\pmod{(x^2-x-1)}$

$a+bx$ のイデアルに $[a,b]$ という2次元ベクトルを考えることもできる。

和の方は $[a,b]+[a',b']=[a+a',b+b']$

乗法は $[a,b][a',b']=[aa'+bb',ab'+b'a]$

x はもはや変数ではなく $x^2=x+1$ をみたす新たな数である

$\mathbb{Q}[x]/(x^2-x-1)$ とは有理数体 $\mathbb{Q}$ なかで

x という数を1個だけ足した閉じた世界

有理数体，実数体，複素数体 → 無限体
では有限体を考える，　素数 p の個数をもつ体 K ← 標数は p

$q \in K$,

$$\underbrace{q+q+q\cdots+q}_{p} = pq + eq + \cdots + eq$$
$$= \underbrace{(e+e+\cdots+e)}_{p} q$$
$e+e+\cdots+e=0$ だから
$$= 0$$

K の加法の群を考えると，これは可換群で素数の累乗を位数とする
巡回群の直和として表される
巡回群の位数はすべて p の累乗、加群の位数は p の累乗

位数 2^n の有限体を考える
$\#_2 = \{0,1\}$，　$n=3$ なら
$a+bx+cx^2 \leftrightarrow (a,b,c)$ で要素を表せる
一般に
$a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1}$
$(a_i \in \{0,1\})$

要素数は 2^n

定理　位数の等しい有限体は同型である

ガロア理論

基礎体 k ⊂ 有限次の分離的な拡大体 Σ

k の既約多項式が Σ の中に1つの根をもてば、
その多項式は Σ の中で完全に1次式の積に分解するものとする。
このような Σ を k に対してガロア拡大体
もしくは正規拡大体という

$\varphi(x)$ を k 上 r 次の既約多項式として、Σ の要素 α を根にもつと

$$\varphi(x) = (x-\alpha)(x-\alpha')\cdots(x-\alpha^{(r-1)})$$

となるから $\alpha', \alpha'', \cdots, \alpha^{(r-1)}$ はすべて Σ に属する。

Σ は有限分離的なので原始要素 θ によって

$$\Sigma = k(\theta)$$

$[\Sigma : k] = n$ とすると、

θ の満足する n 次の既約多項式を $f(\theta)$ とすると

$$f(x) = (x-\theta)(x-\theta')\cdots(x-\theta^{(r-1)})$$

となり $\theta, \theta', \cdots \theta^{(r-1)}$ はすべて Σ に属する

k の要素を動かさず Σ の要素を自己同型に写す p とすると

$\alpha, \beta \in \Sigma$ のとき $\quad p(\alpha \pm \beta) = p(\alpha) \pm p(\beta)$

$$p(\alpha\beta) = p(\alpha)p(\beta)$$

$q \in k$ に対して $\quad p(q) = q$

また $\quad p(\theta) = q_0\theta^n + q_1\theta^{n-1} + \cdots + q_n = 0$

$$\Longleftrightarrow p(q_0\theta^n + q_1\theta^{n-1} + \cdots + q_n) = p(0)$$

$$\Longleftrightarrow p(q_0\theta^n) + p(q_1\theta^{n-1}) + \cdots p(q_n) = 0$$

$$\Longleftrightarrow p(q_0)p(\theta^n) + p(q_1)p(\theta^{n-1}) + \cdots p(q_n) = 0$$

$q_0, q_1 \cdots q_n \in k$ だから $p(q_i) = q_i$

$$q_0 p(\theta^n) + q_1(\theta^{n-1}) + \cdots q_n = 0$$

多項式の形

$p(\theta)$ は $\varphi(x) = 0$ の根、
すなわち $\theta, \theta', \theta'', \cdots \theta^{(n-1)}$ のうちの1つ

$$p(\theta) = \theta^r$$

つまり p は θ を共役数の1つに置きかえる

---

p は θ と同じ方程式の別の解に
入れ替えるだけの操作

$p_0(\theta) = \theta$
$p_1(\theta) = \theta'$
$\vdots$
$p_{n-1}(\theta) = \theta^{(n-1)}$ となる n 個の自己同型がある

$\forall \alpha \in \Sigma = k(\theta)$, θ の有理式 $f(\theta)$ により

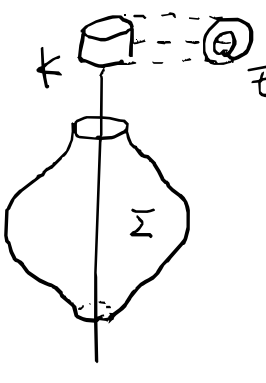
$$\alpha = f(\theta)$$

$$\Longleftrightarrow p(\alpha) = p(f(\theta)) = f(p(\theta))$$

p は Σ のすべての要素の自己同型を引き起こす

この自己同型全体は群をなす
これをガロア拡大体 Σ/k の**ガロア群**という

位数は Σ/k の拡大次数に等しい



モーターがロア群

中心線 k
回転体 Σ ← k のまわりに自由に回転

モーターを回すと Σ の中の θ は
$\theta', \theta'', \cdots \theta^{r-1}$ に巡る

基本定理　1. Σ と K の中間にある体 Δ ($\Sigma \supseteq \Delta \supseteq K$) を
動かさないような Ω 群の要素全体の集合は
G の部分群 H である。またこの H によって動かされない
ような Σ の要素全体はもとの Δ に一致する。

2. 逆に G の部分群 H によって動かされない Σ の要素
全体は Σ の部分体をなし、この部分体を動かさない
G の要素の全体はもとの H に一致する。

$G \to G'$ に準同型写像したときに、部分群 H とすると $G/H \cong G'$ となった
単純群とは、$G/G \cong E$, または $G/E = G$ となる群 G のことで
準同型において これ以上縮小できない。整数の中での素数のような
存在

群 G が単純でないとは G より小さくて単位群でない正規部分群 G_1
がある　$G \supset G_1$
同じように $G_1 \supset G_2$ がありえる
$G = G_0 \supset G_1 \supset \cdots G_l = E$

G_i は G_{i-1} の正規部分群になっている。
G_{i-1}/G_i をこの列の因子という。
l をこの列の長さという。
列のあいだに別の群を割り込ませる余地がないほど
細かくなっている列を組成列という。

$G_{i-1}/G_i = G'$ が単純でないとすれば、G'
のなかには G' と単位群 E のあいだに正規部分群 H がある。
ここで $G_{i-1} \to G'$ という準同型写像で H に
写される G の要素の全体は G_{i-1} のなかの正規部分群
となる。
この群は G_{i-1} と G_i の中間にある正規部分群であるから
上の列は組成列ではなくなる。$\therefore G_{i-1}/G_i$ は単純である。

定理　$G = G_0 \supset G_1 \cdots \supset G_l = E$ が組成列をなすためには、
その因子群 G_0/G_1, G_1/G_2, $\cdots$ G_{l-1}/G_l
がすべて単純であることが、必要かつ十分である。

定理　G の二つの組成列を
$G = G_0 \supset G_1 \supset \cdots \supset G_r = E$
$G = H_0 \supset H_1 \supset \cdots \supset H_s = E$
とすると、その因子群は適当に順序を変えると、
1つずつ同型である

S_4 の4つの元に $1, 2, 3, 4$ を2つ2に分けて、その入れ方を
入れ換える置換の全体を考えると

クラインの4元群

V_4　(1), $(1,2)(3,4)$, $(1,3)(2,4)$, $(1,4)(2,3)$
V_4 は群をつくる
すべて偶置換だから $V_4 \subset A_4$

V_4 は S_4 の正規部分群
V_4 で $(1) = e$, $(1,2)(3,4) = a$, $(1,3)(2,4) = b$
とすると　$ab = (1,4)(2,3)$, $ba = (1,4)(2,3)$
$a^2 = e$, $b^2 = e$
V_4 は $(2,2)$ 型の可換群
ここで $(e, a) = C_2$ とすると S_4 の組成列は
$S_4 \supset A_4 \supset V_4 \supset C_2 \supset E$
その因子群の位数は $2, 3, 2, 2$
したがって S_4 は可解

$x^2+px+q=0$

$x_1-x_2=\sqrt{D}$

$D=(x_1-x_2)^2$

$=(x_1+x_2)^2-4x_1x_2$

$=p^2-4q$

ヴィエタの公式

$x_1+x_2=-\frac{p}{1}=-p$

$x_1x_2=\frac{q}{1}=q$

$x_1=\sqrt{D}+x_2$

$x_1=-p-x_2$

$\sqrt{D}+x_2=-p-x_2$

$2x_2=-p-\sqrt{D}$

$x_2=\frac{-p-\sqrt{D}}{2}$

$x_1=-p+\frac{p+\sqrt{D}}{2}$

$=\frac{-p+\sqrt{D}}{2}$

ヒアリング. 構造の条件

1. 全体性
2. 変換性
3. 自己制御

$x \to ax=y$

$x \to axa^{-1}$

変換は構造に関じる

あるいは構造を広く大きく

閉じるようにする