B3　代数系とその応用

【置換群】

置換 $\begin{pmatrix}1 & 2 & \cdots & n\\ j & k & \cdots & l\end{pmatrix}$ を {j, k, …, l} で表わす。

ｎを与えて、ｎ次の置換をランダムに１つ発生させよ。

与えられたリストが置換であるか否か判定すること。

n を与えて（例えば n=5)、ｎ次対称群とｎ次交代群の要素を表示させよ。

任意の置換 a=$\begin{pmatrix}1 & 2 & \cdots & n\\ i_1 & i_2 & \cdots & i_n\end{pmatrix}=\{i_1 \quad i_2 \quad \cdots \quad i_n\}$ を巡回置換の積であらわせ。

長さ３と長さ２と長さ１の巡回置換の積は　{{j,k,l},{p,q},{r}} のように表わす。

逆に、巡回置換の積を元の置換に戻すこと。

```
<<DiscreteMath`Permutations`
PermutationQ[{1,2,3}]
PermutationQ[{1,2,2}]
RandomPermutations[10]
ToCycles[%]
FromCycles[%]
```

ｎを定めて

２つの置換 a,　b の積を計算する関数 seki[n,a,b] を作れ。

置換 a の逆置換 を計算する関数 inv[n,a] を作れ。

置換 a のm乗を計算する関数 beki[n,a,m] を作れ。

置換 x を与えて、ｘで生成した巡回群を作成する cyc[n,x] を作れ。

巡回置換が与えられたとき、その中の最大の文字を探して、置換への表現

{1,4,3} -> {{1,4,3},{2}} -> {4,2,1,3}

のようにする関数　toStdPer[a] をつくる。

【行列群】

Ｋを実数体Ｒまたは複素数体Ｃのいずれかとする。Ｋの元を成分とするｎ次行列全体のうち、正則行列の全体のなす群は一般線形群と呼ばれ GL(n, K) で表し、特に行列式の値が１であるような行列全体の作る部分群は特殊線形群と呼ばれ SL(n, K) で表す。Ｋ＝Ｒ

の場合、ｎ次の直交行列全体のなす群は直交群といい O(n) で表す。またＫ＝Ｃの場合、ｎ次ユニタリ行列全体の作る群はユニタリ群といい、U(n) で表す。

$G=\left\{\begin{pmatrix}1 & a & b\\ 0 & 1 & c\\ 0 & 0 & 1\end{pmatrix} \mid a,b,c\in R\right\}$ は GL(3, R) の部分群であることを示せ。

$W=\{w_0,w_1,w_2,w_3,w_4,w_5\}$ は行列の積について GL(3, R) の部分群であることを示せ。ただし、 $w_0=\begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix}$ $w_1=\begin{pmatrix}0 & 1 & 0\\ 1 & 0 & 0\\ 0 & 0 & 1\end{pmatrix}$ $w_2=\begin{pmatrix}1 & 0 & 0\\ 0 & 0 & 1\\ 0 & 1 & 0\end{pmatrix}$

$w_3=\begin{pmatrix}0 & 0 & 1\\ 1 & 0 & 0\\ 0 & 1 & 0\end{pmatrix}$ $w_4=\begin{pmatrix}0 & 1 & 0\\ 0 & 0 & 1\\ 1 & 0 & 0\end{pmatrix}$ $w_5=\begin{pmatrix}0 & 0 & 1\\ 0 & 1 & 0\\ 1 & 0 & 0\end{pmatrix}$ とする。

$A(t)=\begin{pmatrix}1 & -t & t\\ t & 1-\frac{t^2}{2} & \frac{t^2}{2}\\ t & -\frac{t^2}{2} & 1+\frac{t^2}{2}\end{pmatrix}(t\in R)$ とおく。 $A(t_1+t_2)=A(t_1)A(t_2)$ を示し、 $A(t)$ の全体は SL(3, R) の部分群であることを示せ。

【いろいろな群】

実数の集合 G = (-1, 1) における積◦を $a\circ b=\frac{a+b}{1+ab}$ で定めると、G は群であることを示せ。

次の変換の集合　$M=\{f_1, f_2, f_3, f_4, f_5, f_6\}$ は変換の積について群であることを示せ。また結合表を作れ。

$f_1(x)=x$,　$f_2(x)=1-x$,　$f_3(x)=\frac{1}{x}$,

$f_4(x)=\frac{1}{1-x}$, $f_5(x)=\frac{x}{x-1}$,　$f_6(x)=\frac{x-1}{x}$

【いろいろな環】

環 $(R,+,\cdot)$ の２元 a,b に対して新しい二項演算 $\oplus,\circ$ を次で定義する。

$$a\oplus b=a+b-1,\ a\circ b=a+b-a\cdot b$$

このとき、$(R,\oplus,\circ)$ はまた環をなすことを示せ。

体Kに対してA＝K×K×Kとおく。

Aの加法は項別に行い、Aにアーベル群の構造を入れる。Aの積は

$$(x_1,x_2,x_3)(y_1,y_2,y_3)=(x_1y_1,x_1y_2+x_2y_1,x_1y_3+x_2y_2+x_3y_1)$$

とする。このとき、Aは可換環である。

体Kに対して、次のような成分を持つ行列の全体は、全行列環の部分環をなす。

$$\mathrm{T}=\left\{\begin{pmatrix}a&0&0\\b&c&0\\d&e&f\end{pmatrix}\middle|\,a,b,c,d,e,f\in K\right\}$$ 簡単に $\begin{pmatrix}K&0&0\\K&K&0\\K&K&K\end{pmatrix}$ と書く。

$$\mathrm{R}=\left\{\begin{pmatrix}a&0&0\\b&c&0\\d&e&a\end{pmatrix}\middle|\,a,b,c,d,e\in K\right\}$$

$$\mathrm{R'}=\left\{\begin{pmatrix}a&0&0\\b&a&c\\d&0&e\end{pmatrix}\middle|\,a,b,c,d,e\in K\right\}$$

$$\mathrm{R''}=\left\{\begin{pmatrix}a&0&0\\b&a&0\\d&0&e\end{pmatrix}\middle|\,a,b,d,e\in K\right\}$$

$$\begin{pmatrix}K&K&K&K\\0&K&0&0\\0&0&K&K\\0&0&0&K\end{pmatrix}\qquad\begin{pmatrix}K&K&K&K\\0&K&0&K\\0&0&K&0\\0&0&0&K\end{pmatrix}\qquad\begin{pmatrix}K&K&0&K\\0&K&K&K\\0&0&K&0\\0&0&0&K\end{pmatrix}$$

$$\mathrm{B}=\left\{\begin{pmatrix} a & 0 & c & d \\ 0 & a & 0 & c \\ 0 & 0 & b & 0 \\ 0 & 0 & 0 & b \end{pmatrix} \middle| a,b,c,d \in K \right\}$$

$$\mathrm{C}=\left\{\begin{pmatrix} a & b & c & d \\ 0 & a & 0 & c \\ 0 & 0 & a & b \\ 0 & 0 & 0 & a \end{pmatrix} \middle| a,b,c,d \in K \right\}$$

T や R のすべてのイデアル、左イデアル、右イデアルを求めよ。

R と R' は環同型であることを示せ。

環 R の２元 a,b に対して $[a,b]=ab-ba$ とおく。このとき

$$[a,[b,c]]+[b,[c,a]]+[c,[a,b]]=0$$

が成立することを示せ。

$[a,b]=ab-ba$ が０で置き換えられぬように注意

標数 p の素体 Z_p の上のｎ次行列環 $R=(Z_p)_n$ について次を示せ。

p と n を指定して（例えば $p=2, n=2$） R のすべての元を表示すること。

R のすべての冪等元を求めること。

R のすべての単元（ここでは正則行列）を求めること。

R の任意の元は、冪等元と単元の和として表されること。

（このような条件を満たす環は clean ring と呼ばれる）

【いろいろな体】

$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}(a,b\in R)$ の全体は C と同型な体をなすことを示せ。

有限体 $GF(p^n)$ を次の場合について構成すること。

p=2，n=2

p=2，n=4

p=5，n=3

【符号理論】

符号理論の概要

通信回線を通してデータを送る際、１つ１つのデータは０または１の数字の列に変換される。０と１からなる集合$F=\{0,1\}$ の ｎ個の直積 F^n を考え、送信するデータをF^nの元に対応させる。データに対応付けられたF^nの元を長さｎの符号語という。符号語の集合を符号(code)または２進符号(binary code)という。データを通信回線を通して送信する際には、途中でデータが変質する可能性を常に考慮しなくてはならない。具体的には、通信の途中でいくつかの０が１に変わり、いくつかの１が０に変わる。送られてきた符号を見て、受信者が自らの判断で誤りを訂正し、元の符号に復元することができるならばデータ通信の際の信頼性は飛躍的に向上する。

誤りの検出に用いられる符号を誤り検出符号、訂正に用いられる符号を誤り訂正符号という。符号理論(coding theory)は、このような誤り検出符号や誤り訂正符号の構成法、その符号化、復号法、符号による誤り訂正検出、訂正の限界、符号を用いたときの信頼性の解析などを扱う理論である。

最小距離

F^nの２つの元$x=(x_1,x_2,...,x_n)$，$y=(y_1,y_2,...,y_n)$に対し、$x_i\neq y_i$となる ｉ の個数をｘとｙのハミング距離(Hamming distance)といい、$d(x,y)$と書く。ハミング距離は距離の公理をみたす。$0=(0,0,...,0)$とｘのハミング距離をｘのハミング重み(Hamming weight)と呼び w(x) と書く。F^nの部分集合Ｃを長さｎの符号(code)と呼ぶ。

$d=\min\{d(x,y);x,y\in C,x\neq y\}$を符号Ｃの最小距離(minimum distance)という。最小距離がｄ である符号に対し $e=\left[\frac{d-1}{2}\right]$とおく。ただし［　］はガウスの記号である。

データの送信途中に誤りが生じた場合、誤りの個所が ｅ 以下であれば、誤りを訂正し正しいデータを復元することができる。

ハミングの上限界式　符号$C(\subset F^n)$について、Ｃの元の数をＭとすると

$$2^n\geq M(1+{}_nC_1+{}_nC_2+\cdots+{}_nC_e)\quad \text{ただし}\ e=\left[\frac{d-1}{2}\right]$$

この公式で等号がなりたつような符号Ｃを完全符号(perfect code)という。完全符号は与えられた長さｎと最小距離ｄをもつ符号の中で、最も符号語の多い符号である。

線形符号

$F=\{0,1\}$ を位数２の有限体とみなす。このときF^nはF 上のｎ次元ベクトル空間であ

る。符号$C(\subset F^n)$がF^nのｋ次元部分空間になっているときＣを長さｎのｋ次元線形符号といい、(n,k)-線形符号と書く。また、最小距離がｄである(n,k)-線形符号を(n,k,d)-線形符号と書く。

以下、Ｃを(n,k,d)-線形符号とする。Ｃはｋ次元ベクトル空間だからＣの中からｋ個の線形独立なベクトルを選ぶことができる。これらベクトルを並べてできるｋ×ｎ行列ＧをＣの生成行列(generator matrix) とよぶ。このとき

$$C = \{xG; x \in F^n\}$$

がなりたつ。また、ＣはF^nのｋ次元部分ベクトル空間だからＣを解空間とするような連立一次方程式が存在する。即ち、階数がn-kであるような n×(n-k) 行列Ｈが存在して

$$C = \{x \in F^n; xH = 0\}$$

と表わすことができる。このような行列ＨをＣのパリティ検査行列(parity check matrix)という。線形符号Ｃに対する生成行列Ｇやパリティ検査行列Ｈは多数あり、一意には定まらないが常にＧＦ＝０がなりたつ。

F^nの元は2^n個ある。このうち、０以外の元をすべて行ベクトルとして並べてできる行列をＨとする。Ｈは $(2^n-1)\times n$ 行列である。

Ｈをパリティ検査行列とする線形符号を<u>ハミング符号</u>(Hamming Code)という。

例　n=3 とする。F^3の元は８個あり、零ベクトルを除いて並べる行列Ｈは

$$H = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

である。$C = \{x \in F^3; xH = 0\}$を求めよ。Ｃ内の一次独立な４個のベクトルを求めよ。

ＣはＨをパリティ検査行列とする(7,4)-線形符号である。

さて、$x = (1,1,1,1,1,1,1) \in C$を送信した際に誤りが生じ、受け手が$y = (0,1,1,1,1,1,1)$を受け取ったとする。ｙはＣの元ではないので送信の際に誤りが生じたことが分かる。Ｃの元の中でｙとのハミング距離がもっとも小さいのはｘである。従って受け手はｙが誤りであることを知り（誤り検出)、元の符号語ｘに復号する（誤り訂正）することができる。

Ｃの任意の２つの元をとり。それらのハミング距離を求めると３以上の値になる。従って符号Ｃの最小距離は３である。またＣの元は１６個であり、等式$2^7 = 16(1+{}_7C_1)$が成り立つから、Ｃは完全符号である。即ち、Ｃは長さ７と最小距離３を持つ符号の中で最も符

号語の多い符号である。一般に、ハミング符号は完全符号である。

巡回符号

Cを線形符号とする。Cの任意の元$(x_1, x_2, ..., x_n)$に対して$(x_n, x_1, ..., x_{n-1})$もCの元になるとき、Cを巡回符号(cyclic code)という。

$a = (a_0, a_1, ..., a_{n-1}) \in F^n$に対して、多項式$f(x) = a_0 + a_1 x + ... + a_{n-1} x^{n-1}$を対応させる。

剰余環　$F[x]/(x^n - 1)$では　$xf(x) = a_{n-1} + a_0 x + a_1 x^2 + ... + a_{n-2} x^{n-1}$であるから、

$b = (a_{n-1}, a_0, ..., a_{n-2})$には$xf(x)$が対応する。こうして巡回符号を剰余環$F[x]/(x^n - 1)$の部分環とみなせる。

任意の$f(x), g(x) \in C, a \in F$に対し

$$f(x) + g(x) \in C, \quad af(x) \in C$$

ならば、Cは線形符号であり、更に

$$xf(x) \pmod{(x^n - 1)} \in C$$

ならば、Cは巡回符号である。

Fは体であるから、$F[x]$は単項イデアル整域である。従って$C = (g(x))$となる$g(x) \in F[x]/(x^n - 1)$が存在する。$g(x)$をCの生成多項式(generator polynomial)という。

$F[x]/(x^n - 1)$での巡回符号のCの生成多項式は$x^n - 1$の約数であるから、これらは$x^n - 1$を因数分解することによって求められる。

例えば

$$x^{15} - 1 = (1 + x)(1 + x + x^2)(1 + x + x^2 + x^3 + x^4)(1 + x + x^4)(1 + x^3 + x^4)$$

である。ここで

$$m_1(x) = 1 + x + x^4, \quad m_2(x) = 1 + x + x^2 + x^3 + x^4$$

とする。$m_1(x)$は原始既約多項式である。$m_1(x) = 0$の１つの解をαとすると、$m_1(x) = 0$の解は$\alpha, \alpha^2, \alpha^4, \alpha^8$であり、$m_2(x) = 0$の解は$\alpha^3, \alpha^6, \alpha^9, \alpha^{12}$である。

$g(x) = m_1(x) \cdot m_2(x)$とおくと$g(x) = 0$の解は$\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^6, \alpha^8, \alpha^9, \alpha^{12}$の８個である。

mを任意の整数とし、nを$2^m - 1$の約数とする。αを$GF(2^m)$上の１の原始n乗根とし、$g(x)$は$x^n - 1$のn-k次の因子であるとする。$g(x) = 0$の根の中に連続したd個の１のn乗根が存在するとき、$g(x)$を生成多項式とする巡回符号の最小距離はd＋１以上である。

この定理の条件をみたす巡回符号を長さn、計画距離d＋１のＢＣＨ符号という。　特にn = 2m-1 のとき、原始BCH符号(primitive BCH code) とよぶ。

先の多項式$g(x)$によって生成される巡回符号は長さ１５、計画距離５の原始BCH符号にな

っている。
さて、$x^8+x^4+x^3+x^2+1=0$ の１つの解をαとする。αを含む $GF(2)$ の拡大体は $GF(2^8)$ と同型になる。ｔを正整数とするとき

$$f(x)=(x-1)(x-\alpha)(x-\alpha^2)\cdots(x-\alpha^{2t-1})$$

を生成多項式とする符号をリードソロモン符号（ＲＳ符号）という。この符号へｔ個の誤りを訂正できる。
例えば　$f(x)=(x-1)(x-\alpha)(x-\alpha^2)(x-\alpha^3)=x^4+\alpha^{75}x^3+\alpha^{249}x^2+\alpha^{78}x+\alpha^6$
の場合は長さ６４の符号になる。この符号はディジタルＶＴＲの誤り訂正符号として使われている。

自己双対符号

$x=(x_1,x_2,...,x_n),\ y=(y_1,y_2,...,y_n)\in F^n$ について内積　$x_1y_1+x_2y_2+..,x_ny_n$　を (x,y) で表わす。F^n の部分空間Ｃに対してその直交補空間 $C^\perp$ を

$$C^\perp=\{y\in F^n\mid (x,y)=0\ (\forall x\in C)\}$$

と定める。Ｃが線形符号であれば、$C^\perp$ も線形符号となる。$C^\perp$ をＣの双対符号(dual code)という。$C^\perp=C$ となる線形符号を自己双対符号(self-dual code)という。自己双対符号Ｃの生成行列Ｇについては　$GG^T=0$　が成り立つ。また $x\in C$ とすると $xx^T=0$ でなければならないので自己双対符号のハミング重みは偶数である。

さて、次の１１×１１行列Ａを考える。

$$A=\begin{pmatrix}1&1&0&1&1&1&0&0&0&1&0\\0&1&1&0&1&1&1&0&0&0&1\\1&0&1&1&0&1&1&1&0&0&0\\0&1&0&1&1&0&1&1&1&0&0\\0&0&1&0&1&1&0&1&1&1&0\\0&0&0&1&0&1&1&0&1&1&1\\1&0&0&0&1&0&1&1&0&1&1\\1&1&0&0&0&1&0&1&1&0&1\\1&1&1&0&0&0&1&0&1&1&0\\0&1&1&1&0&0&0&1&0&1&1\\1&0&1&1&1&0&0&0&1&0&1\end{pmatrix}$$

１２次の単位正方行列 E_{12} を用いて

$$B=\begin{pmatrix}&&&1\\&A&&\vdots\\&&&1\\1&\cdots&1&0\end{pmatrix},\quad G=(E_{12},B)$$

と定める。Gは 12×24 行列となる。Gを生成行列とする長さ２４の線形符号を拡張 Golay 符号(extended Golay code)という。この符号は誤り訂正能力が高いため惑星探査衛星からの写真データ伝送のための符号としてボイジャー１号、２号で用いられた符号である。拡張 Golay 符号は自己双対符号であり、その最小距離は８である。

参考書

土川真夫　行列と群　現代数学社　１９８０
高木和久他　工学系に必要とされる数学に関する調査研究５
－情報系分野（符号理論）における数学　日本数学教育学会高専部会　１９９８
今井秀樹　符号理論　電子情報通信学会　１９９０
平松豊一　応用代数学・第４章符号理論入門　裳華房　１９９７