数理工学（テキスト）

担当：松田　修

目次

はじめに 4
第 1 週 4
　1．魔方陣 4
　2．ラテン方陣とオイラー方陣 4
　3．n 次の魔方陣に挑戦！ 5
第 2 週 7
　1．体 7
　2．有限体 $\mathbb{Z}_2$ について 7
　3．アファイン平面 $\mathbb{Z}_3 \times \mathbb{Z}_3$ 8
　4．有限体 $\mathbb{F}_4$ について 9
　5．アファイン平面 $\mathbb{F}_4 \times \mathbb{F}_4$ 9
第 3 週 11
　1．４次の魔方陣 11
　2．実験計画法 12
　3．麻雀対戦相手組み合わせの問題 13
第 4 週 14
　1．整数について 14
　2．剰余の計算 15
第 5 週，第 6 週 16
　1．はじめに 16
　2．因数分解について 16
　3．RSA による暗号化と解読法 16
第 7 週，第 8 週 18
　1．射影平面について 18
　2．射影平面上の曲線 18
　3．楕円曲線暗号について 19
第 9 週 21
　1．符号理論について 21
　2．線形符号 21
　3．ハミング距離 21
　4．生成行列 22
　5．パリティー検査 23
第 10 週，第 11 週 25
　1．ハミング符号 25
　2．完全符号 25
　3．巡回符号 25
　4．巡回符号の生成行列とパリティー検査行列 27
第 12 週 29
　1．フーリエ級数の復習 29
　2．ＤＥＦ 30
第 13 週 31
　2^n 点ＦＦＴ 31
　　1．4 点ＦＦＴ 31
　　2．８点ＦＦＴ 33
第 14 週，第 15 週 36
　1．ビットリバーサル 36
　2．ＦＦＴの数理 36

はじめに

本テキストは，「佐藤肇，一楽重雄著，幾何の魔術（日本評論者）」，「桂利行著，代数幾何入門（共立出版）」，「藤原良，神保雅一著，符号と暗号の数理（共立出版）」，「松尾博著，やさしいフーリエ変換（森北出版）」等の本からその内容を一部抜粋して使用しています。

第１週

１．魔方陣

0	4	8
5	6	1
7	2	3

上の図は，縦の列も横の列もその和 12 です。このように縦の列も横の列もその和が一定になる正方形の数の表（方陣）を**魔方陣**といいます。上の魔方陣は 3×3 の方陣なので，3 次の魔方陣といいます。一般に $n \times n$ 方陣の魔方陣を n 次の魔方陣といいます。

＊本講座では，このような魔方陣の作り方をマスターすることから始めて，数学の考え方やスタイルを理解し，それを応用していくことを目的とします。

[問題]　5 次の魔方陣をつくれ。

２．ラテン方陣とオイラー方陣

n 次の魔方陣を作るためにラテン方陣と呼ばれるものを考えます。

ラテン方陣とは，縦の各列も横の各列も同じ数字が一回しか出てこない方陣のことです。下の表を見てください。

0	1	2
1	2	0
2	0	1

（表１）

0	1	2
2	0	1
1	2	0

（表２）

（表１）は，0,1,2 という数字を左にスライドさせて次の行を作っています。（表２）は，右にスライドさせて次の行を作ったものです。

この 2 つの方陣を組み合わせた方陣が次の表です。

(0,0)	(1,1)	(2,2)
(1,2)	(2,0)	(0,1)
(2,1)	(0,2)	(1,0)

上の方陣を**オイラー方陣**といいます。そして上のオイラー方陣は２つのラテン方陣からつくられました。このように２つのラテン方陣を組み合わせてオイラー方陣になるとき，２つのラテン方陣を互いに直行するラテン方陣といいます。

3 次のオイラー方陣とは，0 から 2 までの数字の組(1,1),(1,2),・・・(3,3)が全て現れる方陣のことです。

次にオイラー方陣のカッコをはずして 3 進表示した表と考えます。すると 3 進法での魔方陣が完成します。

0	11	22
12	20	1
21	2	10

これを十進法に直すのです。

0	4	8
5	6	1
7	2	3

最初の魔方陣ができました。

３．*n* 次の魔方陣に挑戦！

上の方法で 4 次の魔方陣を作ってみましょう。

0	1	2	3
1	2	3	0
2	3	0	1
3	0	1	2

（表３）

0	1	2	3
3	0	1	2
2	3	0	1
1	2	3	0

（表４）

(0,0)	(1,1)	(2,2)	(3,3)
(1,3)	(2,0)	(3,1)	(0,2)
(2,2)	(3,3)	(0,0)	(1,1)
(3,1)	(0,2)	(1,3)	(2,0)

（表５）

オイラー方陣を作るときに，同じ組が出てきて失敗です。実は 4 次の魔方陣は全く別の方法でやらなくてはいけないのです。それは次回説明します。

５次の魔方陣を作ってみましょう。

0	1	2	3	4
1	2	3	4	0
2	3	4	0	1
3	4	0	1	2
4	0	1	2	3

（表６）

0	1	2	3	4
4	0	1	2	3
3	4	0	1	2
2	3	4	0	1
1	2	3	4	0

（表７）

(0,0)	(1,1)	(2,2)	(3,3)	(4,4)
(1,4)	(2,0)	(3,1)	(4,2)	(0,3)
(2,3)	(3,4)	(4,0)	(0,1)	(1,2)
(3,2)	(4,3)	(0,4)	(1,0)	(2,1)
(4,1)	(0,2)	(1,3)	(2,4)	(3,0)

（表８）

0	11	22	33	44
14	20	31	42	3
23	34	40	1	12
32	43	4	10	21
41	2	13	24	30

（表９）

（表９）は５進法の表です。それを十進法で書き換えます。

0	6	12	18	24
9	10	16	22	3
13	19	20	1	7
17	23	4	5	11
21	2	8	14	15

（表１０）

【練習１】７次の魔方陣をつくれ。

【課題１】なるべく大きな魔方陣をつくれ（２１次以上)。
【課題２】奇数次のオイラー方陣は上の方法で作ることが可能である。そのことを示せ。

第２週

１．体

加減乗除がうまくいっている集合を**体**（field）といいます。まずその説明から入ります。

（１） 群について

集合Gが**半群**（semi group）であるとは，Gの中に何かある演算$*$が定まっていて，次の条件①を満たすときをいいます。

① $x,y,z\in G$のとき，$x*(y*z)=(x*y)*z$が成り立つ。

さらに，半群Gが**群**（group）であるとは，次の条件（２）（３）を満たすときをいいます。

② 任意の元$x\in G$に対して，$x*e=e*x=x$となる$e\in G$が存在する。

③ 任意の元$x\in G$に対して，$x*x'=x'*x=e$となる$x'\in G$が存在する。

②のeを**単位元**(unit)といっています。③のx'をxの**反対元**といっています。Gの任意の元x,yに対して$x*y=y*x$が成り立つとき，Gを**可換群**(commutative group)といいます。

例１　整数全体の集合$\mathbb{Z}$は足し算で群となります。

例２　実数全体の集合$\mathbb{R}$は足し算でも掛け算でも群となります。

例３　n行列n行列で行列式が０でないもの全体の集合$GL(n)$は掛け算で群となります。

（２） 体について

集合Fが**体**であるとは，Fの中に何かある２つ演算$+$と$*$が定まっていて，次の条件①，②③を満たすときをいいます。

① Fは$+$について可換群である。

② Fは$*$について可換群である。

③ Fの任意の元x,y,zについて$x*(y+z)=(x*y)+(x*z)$が成り立つ。

たとえば，有理数全体は体で，それを**有理数体**といいます。実数全体も体で，**実数体**といいます。しかし整数全体は体ではありません。それは，$1\div 2$などが整数にならないからです。有理数体や実数体はその集合の元の個数が無限にあります。ここでは元の集合が有限な体，**有限体**について学んでいきます。

２．有限体$\mathbb{Z}_2$について

有限体$\mathbb{Z}_2$とは，整数全体を２で割った時の余りによる集合のことです。したがって，$\mathbb{Z}_2$の元は，０と1のみということになります。その足し算と掛け算表は以下になります。

足し算	0	1
0	0	1
1	1	0

（表１）

掛け算	0	1
0	0	0
1	0	1

（表２）

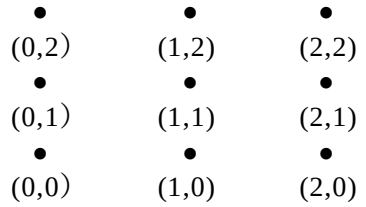
上の表をみて分かるとおり確かに$\mathbb{Z}_2$は四則演算がうまくいっています。

次に整数全体を３で割った時の余りによる集合$\mathbb{Z}_3$を考えます。$\mathbb{Z}_3$の元は，０と1と２で出来ている集合です。これを体になります。確かめてください。

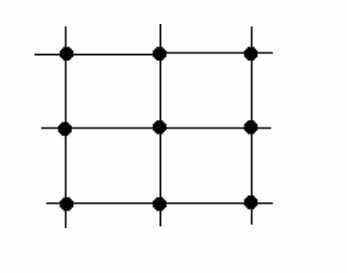
一般にnで割った余りによる集合は体にはなりません。しかし，素数pで割った余りによる集合$\mathbb{Z}_p$は体になります。

３．アファイン平面$\mathbb{Z}_3\times\mathbb{Z}_3$

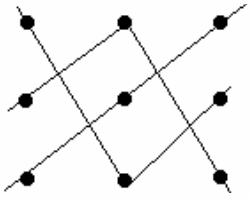
アファイン平面$\mathbb{Z}_3\times\mathbb{Z}_3$とは，いわゆる$x$軸と$y$軸に 0,1,2 の座標をとったものを考えます。したがって下の図のように９つの点しか存在しません。



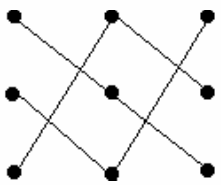
さて次に$\mathbb{Z}_3\times\mathbb{Z}_3$での直線を考察します。直線とは，$y=ax+b$または$x=c$を満たす点の集合のことです。
まず，$x=0,\ x=1,\ x=2$の 3 本の直線が存在します。次に，$y=0,\ y=1,\ y=2$の 3 本の直線があります。



次に，$y=x$を考えると，この直線は点$(0,0),(1,1),(2,2)$を通ります。
$y=x+1$を考えると，これは，点$(0,1),(1,2),(2,0)$を通ります。
$y=x+2$を考えると，これは，点$(0,2),(1,0),(2,1)$を通ります。



次に，$y=2x$を考えると，この直線は点$(0,0),(1,2),(2,1)$を通ります。
$y=2x+1$を考えると，これは，点$(0,1),(1,0),(2,2)$を通ります。
$y=2x+2$を考えると，これは，点$(0,2),(1,1),(2,0)$を通ります。



４．有限体$\mathbb{F}_4$について

整数全体を 3 で割った時の余りによる集合$\mathbb{Z}_4$は体にはなりません。それは，$2\times x=1$となるxが存在しないから割り算ができないからです。しかし４つの元からなる集合を体にすることはできます。それが，有限体$\mathbb{F}_4$なのです。

$\mathbb{F}_4$を説明します。$\mathbb{F}_4$はその部分集合に$\mathbb{Z}_2$を持っています。したがって$\mathbb{F}_4$は$\mathbb{Z}_2$の演算を保持したまま拡大しています。$\mathbb{F}_4$は$\{0,1,\alpha,1+\alpha\}$という４つの元から出来ています。ここで，αは，$\alpha^2+\alpha+1=0$を満足します。したがって，$\alpha^2=-(1+\alpha)=1+\alpha$でもあります。その演算は下図のようになります。

足し算	0	1	α	$1+\alpha$
0	0	1	α	$1+\alpha$
1	1	0	$1+\alpha$	α
α	α	$1+\alpha$	0	1
$1+\alpha$	$1+\alpha$	α	1	0

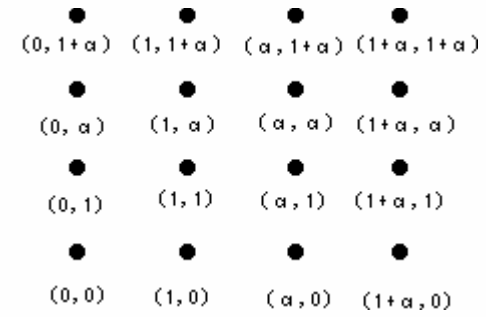
（表３）

掛け算	0	1	α	$1+\alpha$
0	0	0	0	0
1	0	1	α	$1+\alpha$
α	0	α	$1+\alpha$	1
$1+\alpha$	0	$1+\alpha$	1	α

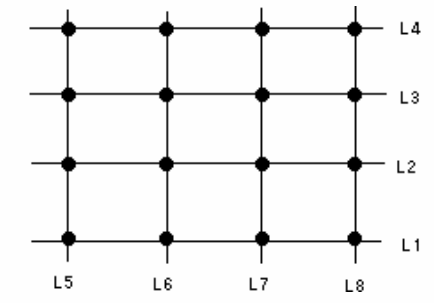
（表４）

５．アファイン平面$\mathbb{F}_4\times\mathbb{F}_4$

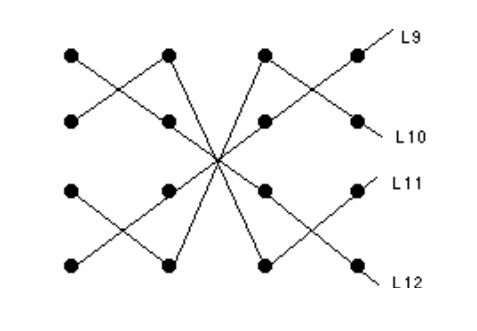
アファイン平面$\mathbb{F}_4\times\mathbb{F}_4$は下図のように 16 個の点で構成された平面のことです。



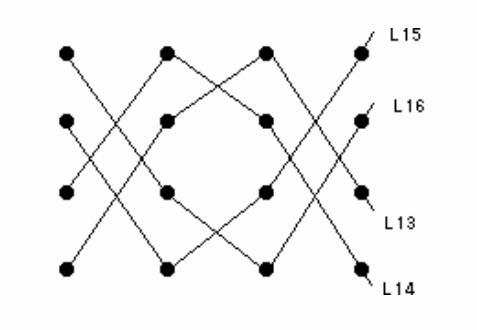
まず，$x=0$，$x=1$，$x=\alpha$，$x=1+\alpha$の４本の直線が存在します。
次に，$y=0$，$y=1$，$y=\alpha$，$y=1+\alpha$の４本の直線があります。
また後々のために下図のように直線に名前をつけておきます。



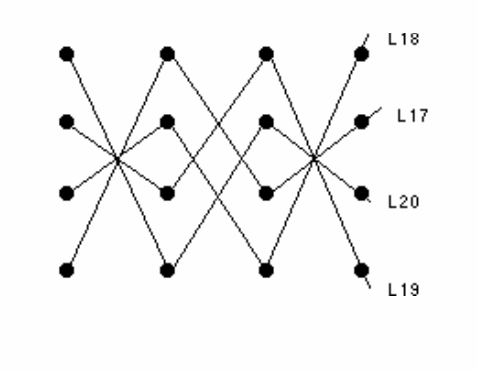
直線$y=x+b$は以下の図のようになります。



直線 $y=\alpha x+b$ は以下の図のようになります。



最後に直線 $y=(1+\alpha)x+b$ は以下の図のようになります。



【練習２】上の直線のグループから２つ選ぶ。例えば｛L9,L10,L11,L12｝と{L17,L18,L19,L20}とする。この中の全ての直線の交点として $\mathbb{F}_4\times\mathbb{F}_4$ の点は全て得られることを確認せよ。

【課題３】$\mathbb{F}_4$ を作るとき，多項式 $\alpha^2+\alpha+1$ を使いました。実はこの多項式は $\mathbb{Z}_2$ を係数とする多項式の中で既約（これ以上因数分解不可能）なものです。３次の既約な多項式の１つに, $1+\beta+\beta^3$ があります。これを使って，$\mathbb{F}_8$ を構成せよ。

第３週

１．４次の魔方陣

前回作ったアファイン平面$\mathbb{F}_4\times\mathbb{F}_4$上の直線は{L1,L2,L3,L4},{L5,L6,L7,L8},
{L9,L10,L11,L12},{L13,L14,L15,L16},{L17,L18,L19,L20}と４つずつにまとめると，各グループはそれぞれ平行な直線達を表しています。さらに重要なことは，２つのグループを選ぶと，その中の全ての直線の交点として$\mathbb{F}_4\times\mathbb{F}_4$の点は全て得られます。

それでは４次の魔方陣の作り方を説明します。

グループを１つ選びます。例えば，{L9,L10,L11,L12}としましょう。まず L9 の通過する点の座標を全て 0 とします。次に L10 の通過する点の座標を全て 1 とします。さらに L11 の通過する点の座標を全て 2 とします。最後に L12 の通過する点の座標を全て 3 とします。次がその表です。

1+α	3	2	1	0
α	2	3	0	1
1	1	0	3	2
0	0	1	2	3
	0	1	α	1+α

（表１）

これよりラテン方陣ができました。

3	2	1	0
2	3	0	1
1	0	3	2
0	1	2	3

（表２）

別なグループを１つ選びます。例えば，{L17,L18,L19,L20}としましょう。先ほどと同様に L17 の通過する点の座標を全て 0 とします。次に L18 の通過する点の座標を全て 1 とします。L19 の通過する点の座標を全て 2 とします。最後に L20 の通過する点の座標を全て 3 とします。次がその表です。

1+α	2	3	0	1
α	1	0	3	2
1	3	2	1	0
0	0	1	2	3
	0	1	α	1+α

（表３）

これよりラテン方陣ができました。

2	3	0	1
1	0	3	2
3	2	1	0
0	1	2	3

（表４）

今作った２つのラテン方陣は直行するので，オイラー方陣を作ることができます。

(3,2)	(2,3)	(1,0)	(0,1)
(2,1)	(3,0)	(0,3)	(1,2)
(1,3)	(0,2)	(3,1)	(2,0)
(0,0)	(1,1)	(2,2)	(3,3)

（表５）

これを４進法で表すと，

32	23	10	1
21	30	3	12
13	2	31	20
0	11	22	33

（表６）

となり，さらに十進法に直すと，

14	11	4	1
9	12	3	6
7	2	13	8
0	5	10	15

（表７）

これで４次の魔方陣が完成しました。

【課題４】８次の魔方陣をつくれ。

２．実験計画法

ある作物の最適な生育環境を調べるための実験を行うことを考えます。いま，土壌の質を３種類，また温度を３段階，湿度も３段階，肥料も３種類，取り替えることができるとします。このとき，どの土壌で，どの温度で，どの湿度で，どの肥料のときに収穫がもっとも多いかを実験で調べてみたいと思います。

簡単に考えつくのは，

$$3^4 = 81$$

通りのすべての環境の床を用意して，すべてを比較することです。しかし，81 通りは多すぎるので，より少ない実験で答えを得ることはできないでしょうか。

環境の相互作用はないとした場合，この問題は 3 次のオイラー方陣で解決されます。

まず，オイラー方陣

(1,1)	(2,2)	(3,3)
(2,3)	(3,1)	(1,2)
(3,2)	(1,3)	(2,1)

を用意します。

オイラー方陣の行は，土壌の 3 種類を意味します。

オイラー方陣の列は，温度の 3 種類を意味します。

そして，オイラー方陣の各成分の前の数字は湿度の種類を意味し，後の数字は肥料の種類を意味するのです。

このようにして，すべての環境がまんべんなく変化した実験の舞台が出来上がります。

さて９つの床の収穫量 S が，上の方陣に対して，

S_{11}	S_{12}	S_{13}
S_{21}	S_{22}	S_{23}
S_{31}	S_{32}	S_{33}

とします。

たとえば土壌１の収穫量の平均は，$\frac{S_{11}+S_{12}+S_{13}}{3}$ となります。

たとえば温度２の収穫量の平均は，$\frac{S_{12}+S_{22}+S_{32}}{3}$ となります。

また湿度３の収穫量の平均は，オイラー方陣の (a,b) において，$a=3$ のところをみればよいので，$\frac{S_{13}+S_{21}+S_{32}}{3}$ となります。

また肥料１の収穫量の平均は，オイラー方陣の (a,b) において，$b=1$ のところをみればよいので，$\frac{S_{11}+S_{23}+S_{32}}{3}$ となります。

３．麻雀対戦相手組み合わせの問題

4 人で行うゲームの対戦相手の組み合わせの問題を考えましょう。16 人が参加し，それぞれの選手が全て他の 15 人とちょうど 1 回ずつ計 5 回プレイするような対戦の組み合わせ表を作れるでしょうか。

一人が 5 回の試合を行い，1 卓に 4 人が参加するのですから，$5\times16/4=20$ 試合です。組み合わせがうまく出来れば 4 試合を行うことができるので，5 ラウンドで全部の試合を行うことができます。

この問題は $4^2=16$ 個の点からなるアファイン平面 $\mathbb{F}_4\times\mathbb{F}_4$ によって解等が得られます。

$\mathbb{F}_4\times\mathbb{F}_4$ 上の直線の考察により，一つの直線は４つの点をもち，平行な直線は 4 本ずつありました。そして平行な直線でグループ分けすると全部で 5 組のグループができました。ですから，最初に $\mathbb{F}_4\times\mathbb{F}_4$ の点に１から１６の番号をつけて，グループ１を第 1 回目の試合とし，各卓を 4 本の平行線によって決めればよいのです。

（$\mathbb{F}_4\times\mathbb{F}_4$ 上の点の番号）

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

	第 1 卓	第 2 卓	第 3 卓	第 4 卓
第 1 回	1,2,3,4	5,6,7,8	9,10,11,12	13,14,15,16
第 2 回	1,5,9,13	2,6,10,14	3,7,11,15	4,8,12,16
第 3 回	1,6,11,16	2,5,12,15	3,8,9,14	4,7,10,13
第 4 回	1,7,12,14	2,8,11,13	3,5,10,16	4,6,9,15
第 5 回	1,8,10,15	2,7,9,16	3,6,12,13	4,5,11,14

【練習３】上のような組み合わせ表を「効率の良い組み合わせ表」と呼ぶことにします。
3 人で行う試合について 9 人が参加する大会の効率の良い組み合わせ表をつくれ。

＊ **第１回レポート提出について。**
【課題１】～【課題４】の中から好きな課題を１つ選んでレポートとして提出せよ。